



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Laboratorio di
Sicurezza Informatica

Sicurezza delle comunicazioni

Marco Prandini

Dipartimento di Informatica – Scienza e Ingegneria

Acknowledgements

- Tutte le slide su richiami di reti locali, vlan, reti IP, routing sono basate su materiali di
 - Franco Callegati <franco.callegati@unibo.it>
 - Walter Cerroni <walter.cerroni@unibo.it>



Outline

■ Richiami di reti

■ Attacchi Passivi

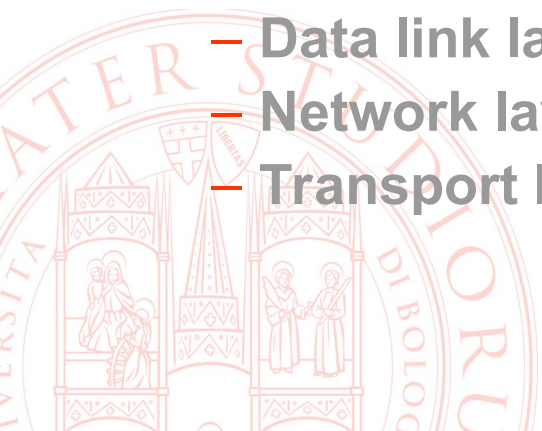
- Scanning
- Sniffing
- Wireless key recovery

■ Attacchi Attivi

- Hijacking ai diversi layer: ARP, BGP, DNS, HTTP
 - e un esempio di come procedere nella kill chain: HTTPS splitting and stripping
- (D)DoS

■ Contromisure: canali sicuri

- Data link layer: VLANs
- Network layer: IPSec
- Transport layer: TLS

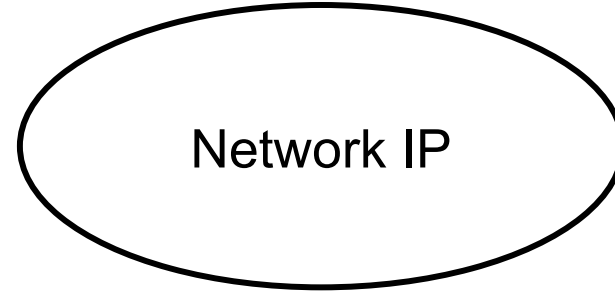


Come funziona Internet

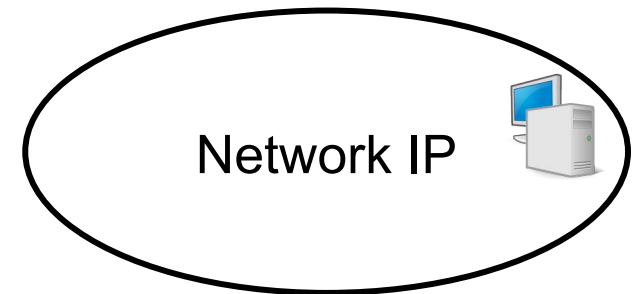
- Internet è una grande “rete di reti”
- La componente elementare è la network IP
 - Ogni network IP è una sorta di isola
 - L’isola tipicamente contiene calcolatori che fungono da nodi terminali della rete detti host
 - Le isole sono interconnesse da apparati che svolgono la funzione di “ponte”
 - Si tratta di calcolatori specializzati detti router o gateway



Internet: reti di reti



Tante Network IP isolate



Indirizzo globale e indirizzo locale

■ Indirizzo globale

- È valido per tutta la rete
- Deve essere **univoco** (non devono esistere indirizzi replicati) per evitare ambiguità
- Va “assegnato” seguendo una procedura di gestione “globale” che assicura la non replicazione

■ Indirizzo locale

- È valido limitatamente ad una certa sottoporzione della rete
 - Internamente ad un terminale
 - In un dominio di rete specifico
- Può non essere globalmente univoco
- Può essere assegnato con una procedura puramente “locale”



Rete logica e rete fisica

- Nella terminologia di Internet si definisce
 - **Rete logica**: la network IP (o **subnet**) a cui un Host appartiene logicamente
 - **Rete fisica**: la rete (tipicamente **LAN**) a cui un Host è effettivamente connesso
- La rete fisica normalmente ha capacità di instradamento e può avere indirizzi locali (es. indirizzi MAC)
- L'architettura a strati nasconde gli indirizzi fisici e consente alle applicazioni di lavorare solo con indirizzi IP



La tecnologia

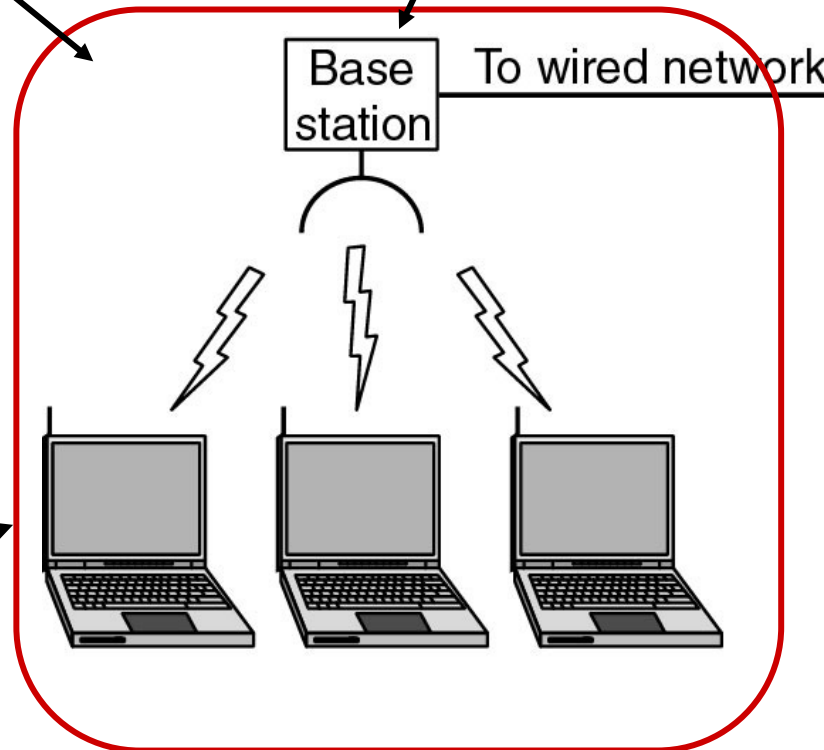
- Ogni network IP può essere implementata con una tecnologia specifica
- Esempio
 - **Wi-Fi** : Network realizzata con tecnologia wireless in area locale
 - **ADSL e xDSL**: Network realizzata con tecnologia a media distanza via cavo tramite infrastruttura di uno specifico fornitore di servizio pubblico
 - **Ethernet**: Network realizzata con tecnologia a breve distanza via cavo privata in area locale
 - **GPRS/EDGE/LTE**: Network realizzata con tecnologia radio a media distanza tramite infrastruttura di uno specifico fornitore di servizio pubblico



Tipica rete wireless: Architettura di rete 802.11

Basic Service Set (BSS)

Access Point (AP)



Distribution System

Wireless Station

Tipica rete cablata: Ethernet basata su SWITCH

- Un bridge è un ponte tra due diverse LAN
- Un bridge tra più di due LAN (ma tipicamente della stessa tecnologia) è denominato HUB
 - Tipicamente ad ogni porta è connessa una sola stazione
- Uno switch Ethernet svolge una funzione simile all'hub ma garantendo maggiori prestazioni
 - È in grado di trasferire contemporaneamente trame da più porte di ingresso a più porte di uscita
 - Opera una funzione di commutazione a livello 2 basata sull'indirizzo MAC



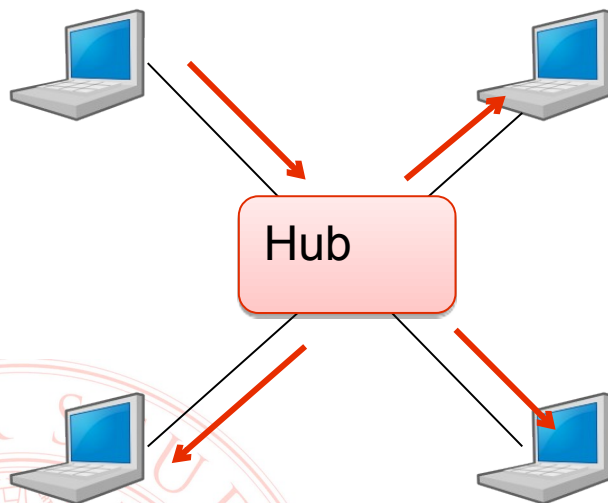
Differenza fra hub e switch

■ Hub

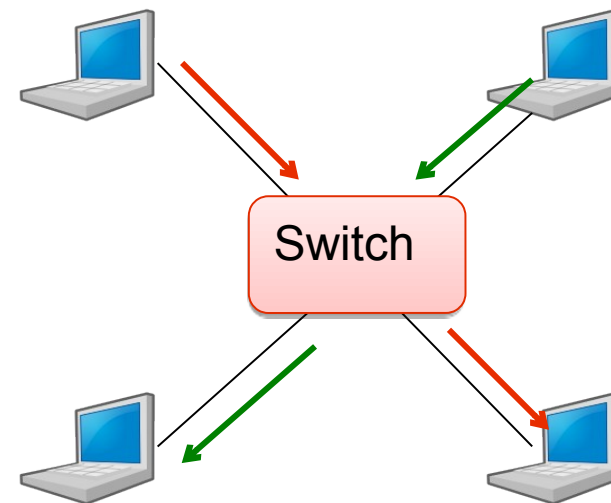
- bus collassato = mezzo condiviso, trasmissione broadcast delle trame
- Capacità aggregata = capacità della singola porta

■ Switch

- Sistema di commutazione = ri-trasmissione selettiva delle trame
- Capacità aggregata superiore a quella della singola porta



Esempio: hub fast ethernet
Si trasferiscono 100 Mbit/s



Esempio: switch fast ethernet
Si trasferiscono 200 Mbit/s

Switch come learning bridge

■ Lo Switch costruisce una “Tabella di inoltro”

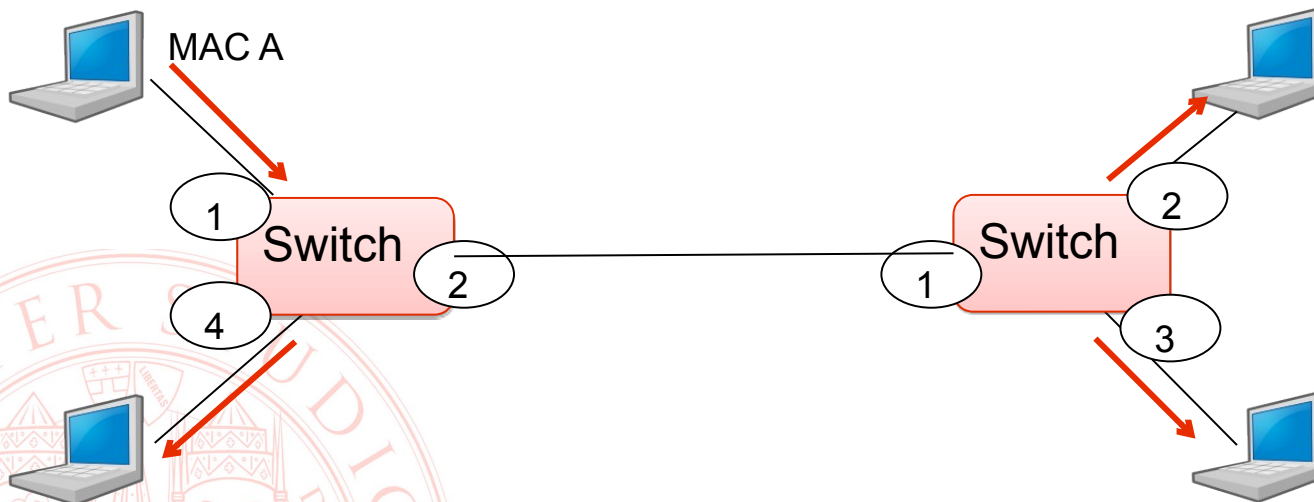
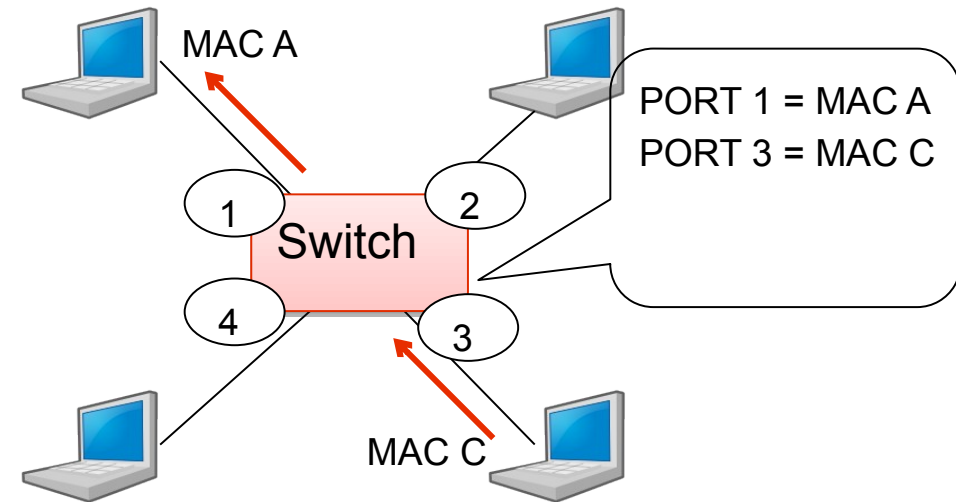
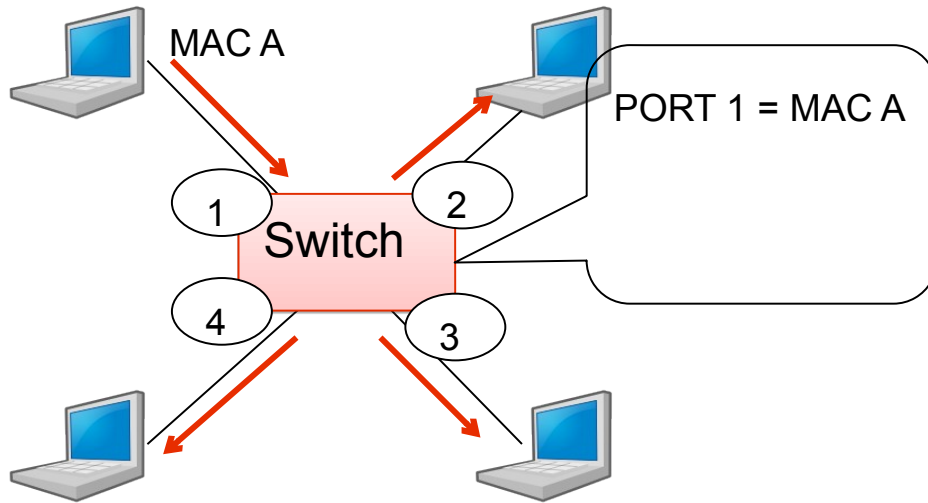
- Associa il Mac Address delle interfacce alla porta dello switch su cui si trova collegata l'interfaccia stessa
- Se alla porta è connesso un altro switch, da essa si raggiungono molteplici MAC di destinazione

■ Esempio switch a 8 porte → implementazione CAM (content addressable mem)

Porta	Lista MAC raggiungibili
1	eb:a6:99:de:1c:b0 2c:65:1e:b1:9f:44
2	
3	0c:2e:22:b0:8e:16
4	
5	
6	5b:06:72:1b:3c:03 e4:b0:56:d5:2d:0f 92:ff:9e:6c:b0:8e
7	
8	

Porta	MAC raggiungibile
1	eb:a6:99:de:1c:b0
1	2c:65:1e:b1:9f:44
3	0c:2e:22:b0:8e:16
6	5b:06:72:1b:3c:03
6	e4:b0:56:d5:2d:0f
6	92:ff:9e:6c:b0:8e

Learning Switch



La network IP

- I calcolatori di una network IP sono connessi dalla medesima infrastruttura di rete fisica (livelli 1 e 2)

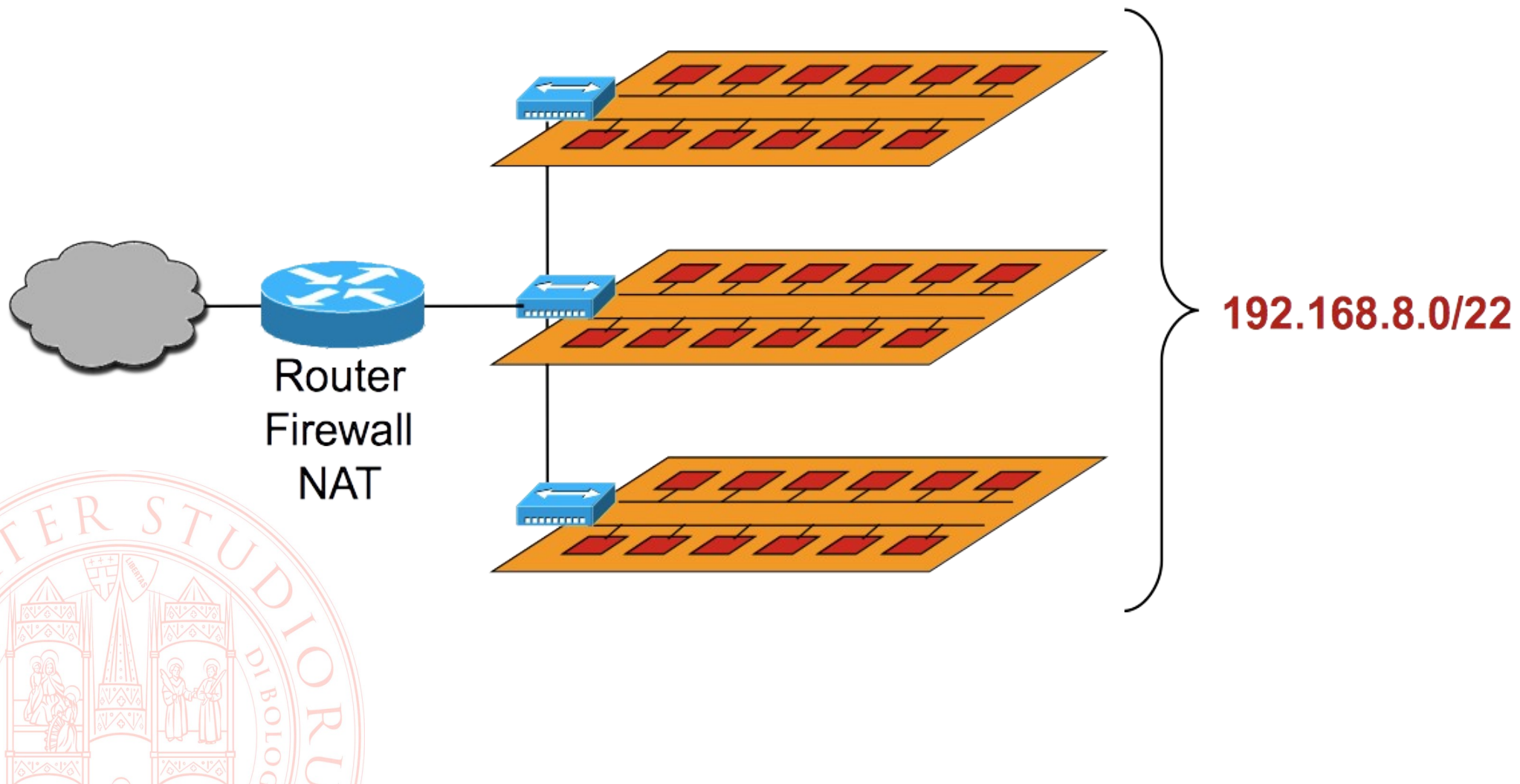
- **Ipotesi fondamentale**

- Tutti gli host appartenenti alla medesima network IP sono in grado di parlare tra loro grazie alla tecnologia con cui essa viene implementata



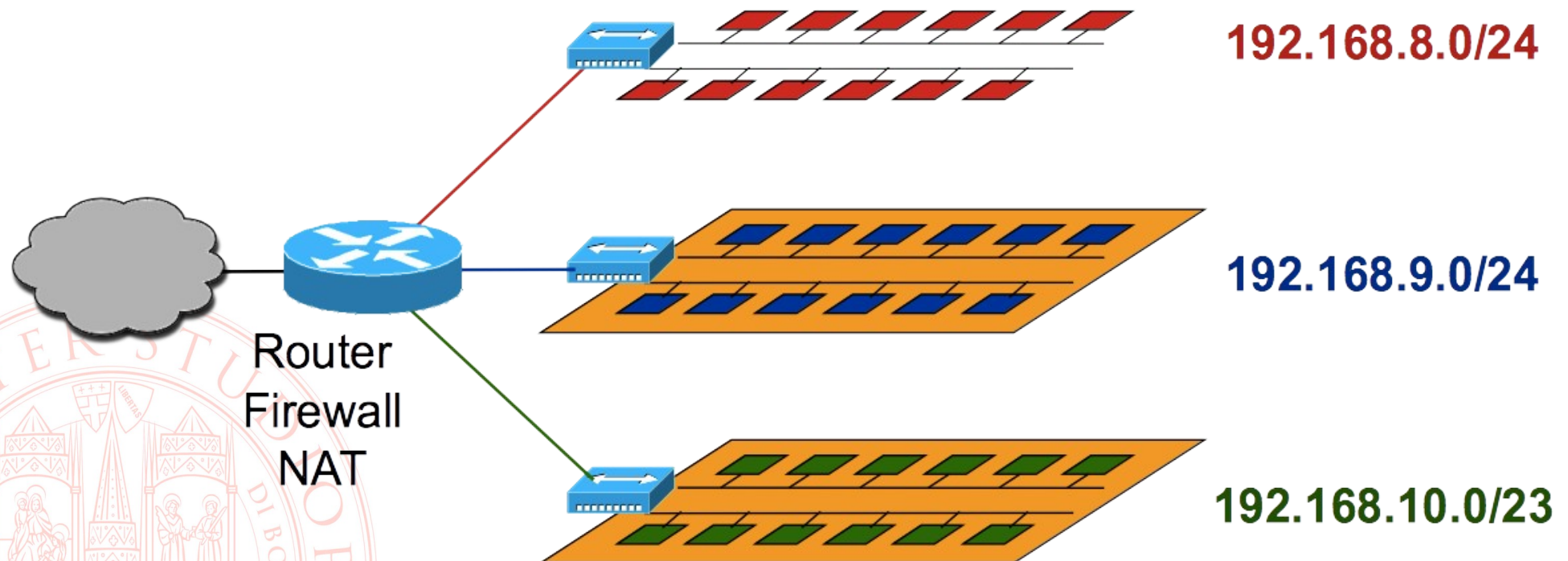
Interconnessione di LAN tramite switch

- Unico dominio broadcast
- Funzionalmente equivalente ad un'unica LAN

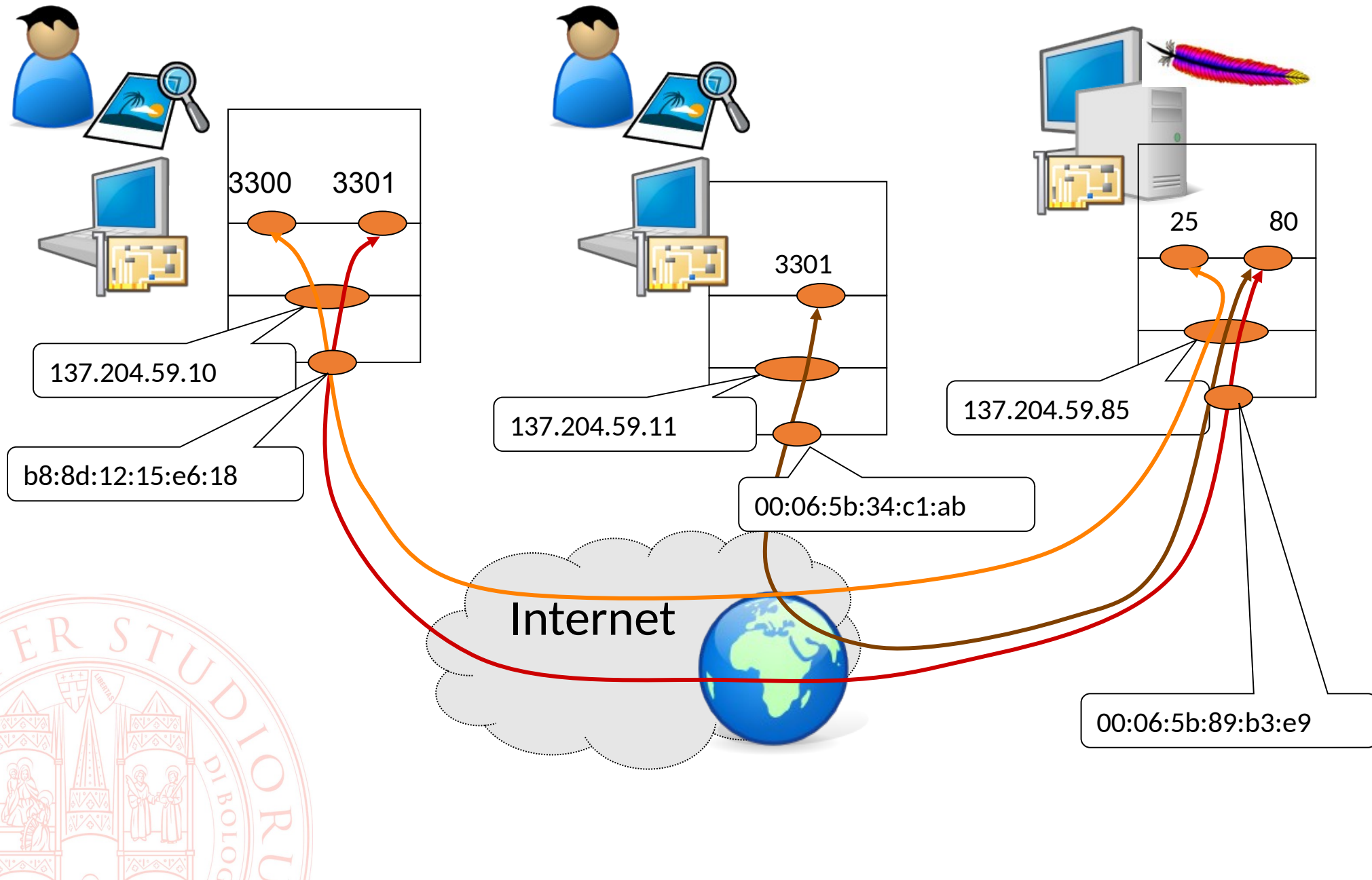


Interconnessione di LAN tramite router

- Domini broadcast separati
- Permette la separazione delle LAN per motivi di
 - efficienza
 - sicurezza
- Limitata mobilità degli host da una LAN all'altra



Flussi di comunicazione



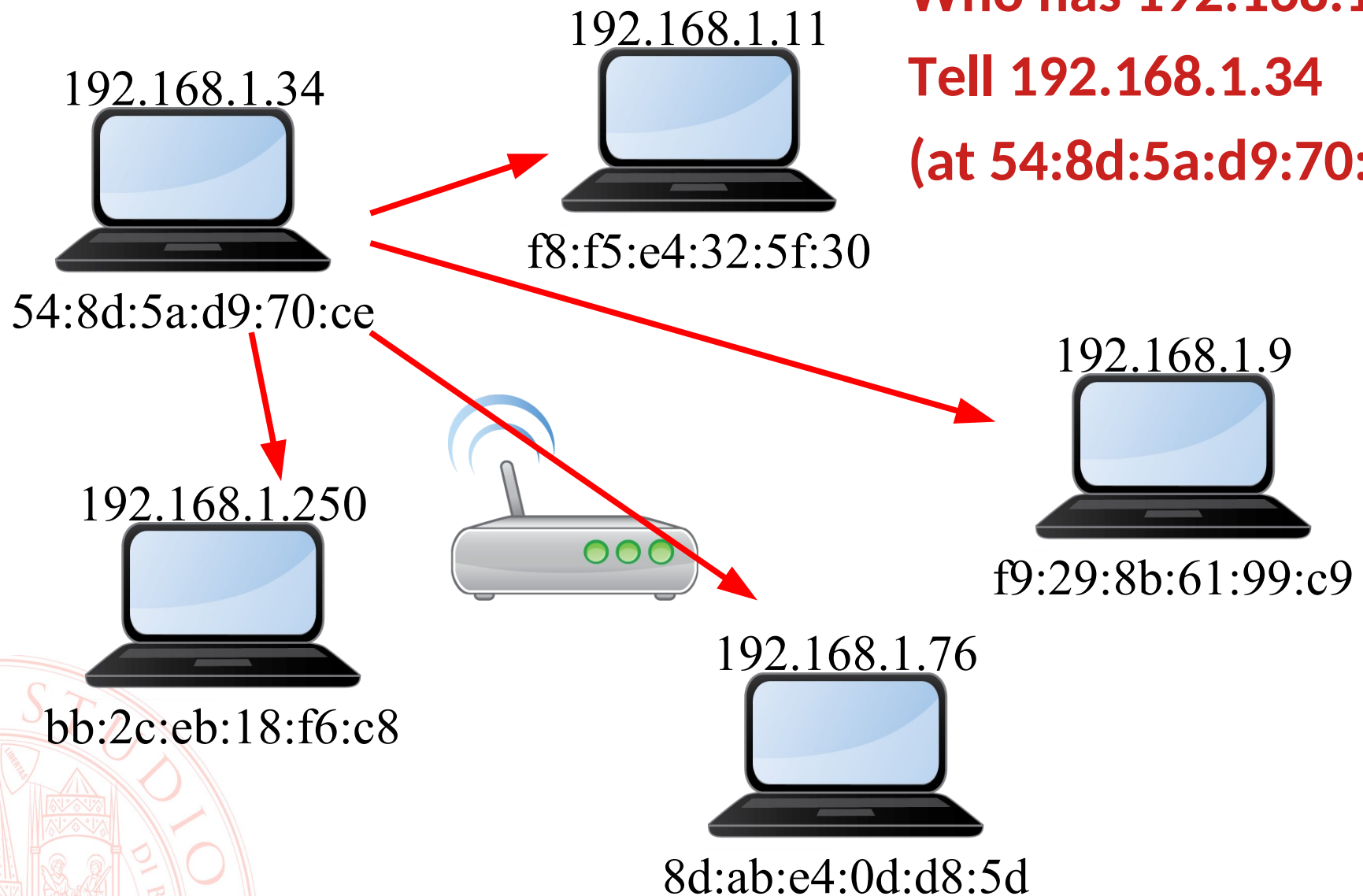
Doppio indirizzamento nella LAN/subnet!

- Ogni dispositivo della LAN ha un MAC address
 - L'inoltro fisico del traffico avviene tra le schede di rete
- Ma è anche un dispositivo della rete IP con un indirizzo
 - Le applicazioni si “conoscono” come endpoint IP
- Come tradurre un indirizzo nell'altro?
- Address Resolution Protocol (ARP – RFC 826)

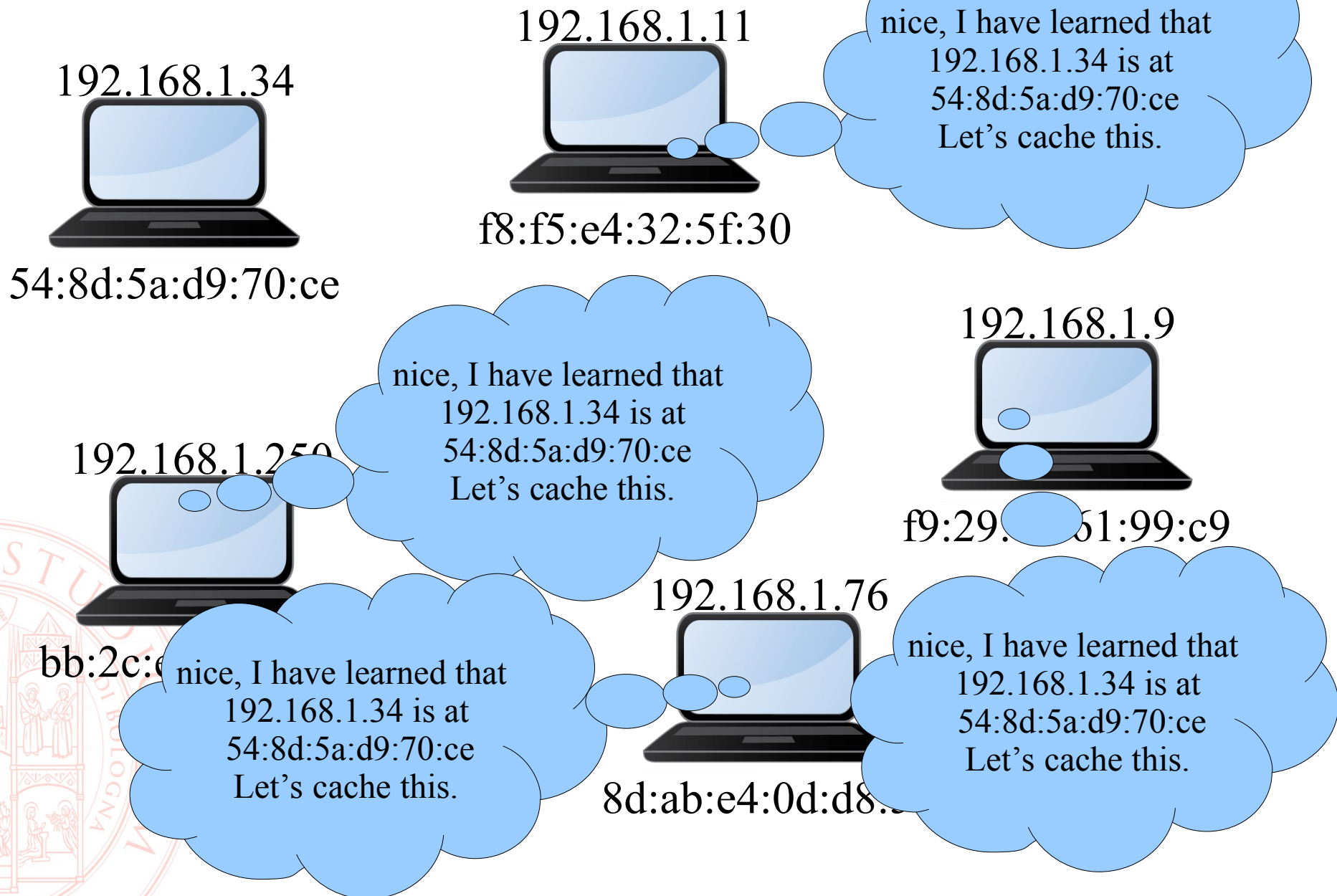


ARP request - broadcast

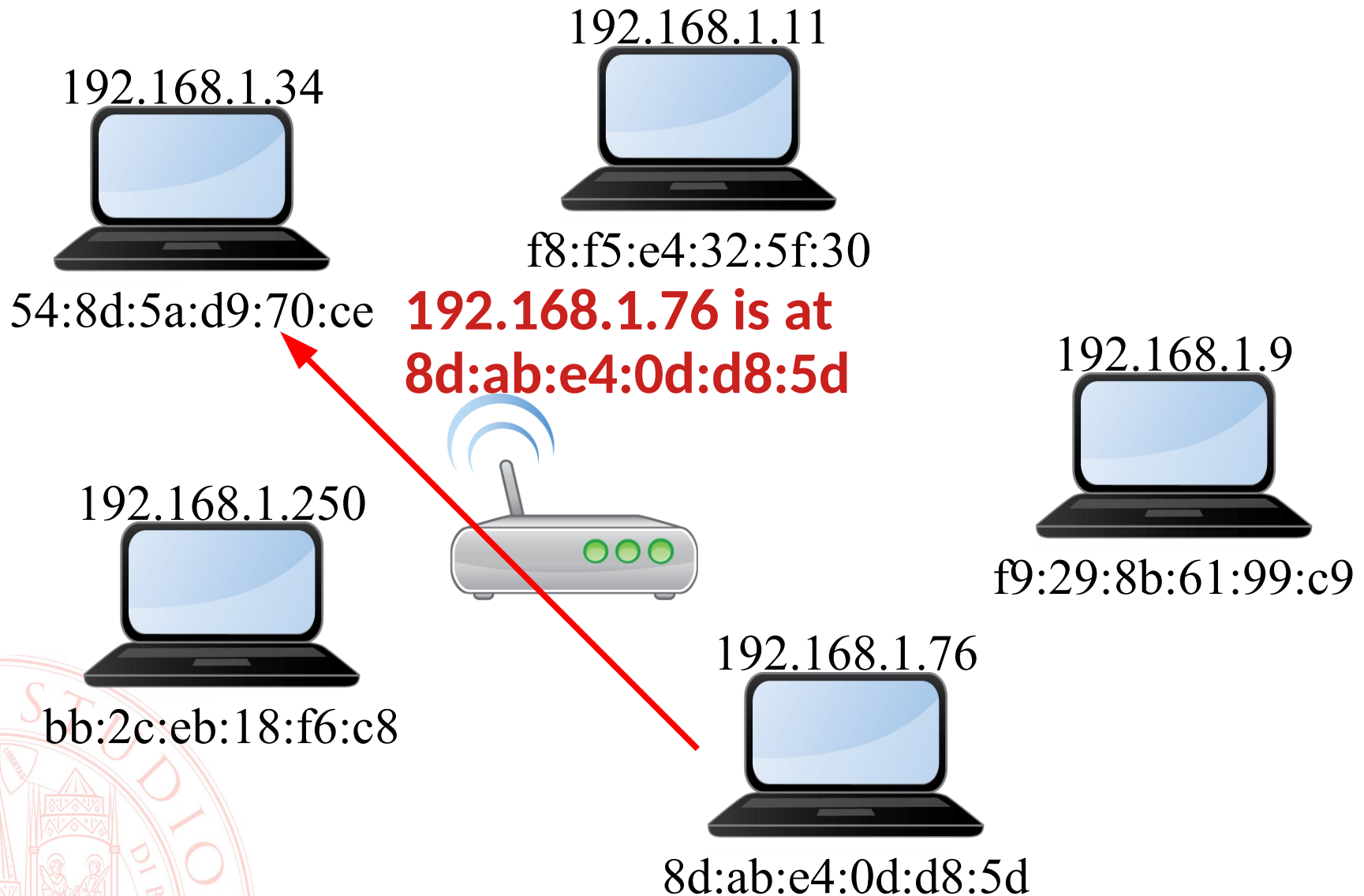
Who has 192.168.1.76?
Tell 192.168.1.34
(at 54:8d:5a:d9:70:ce)



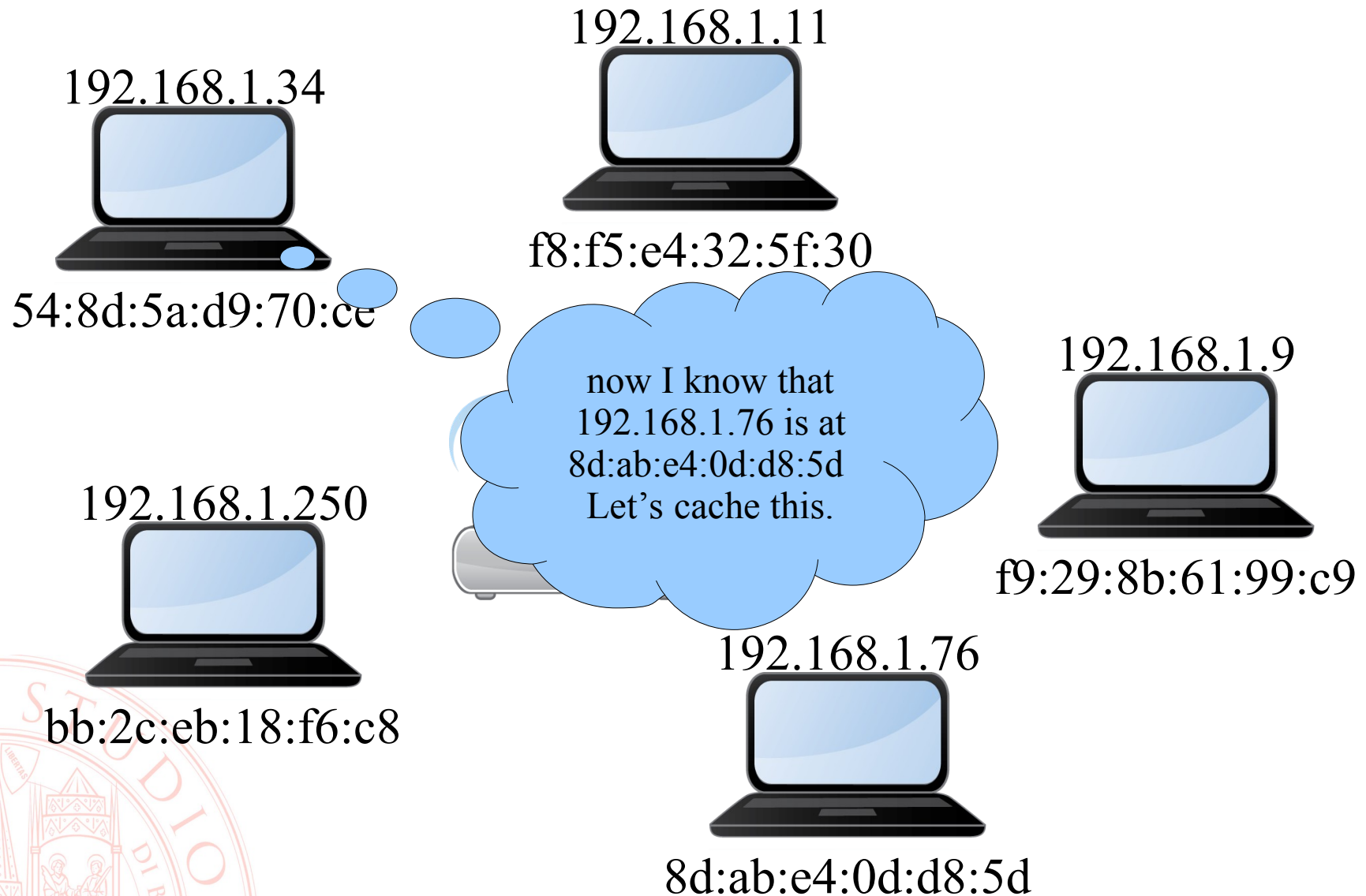
ARP request – caching opportunistic



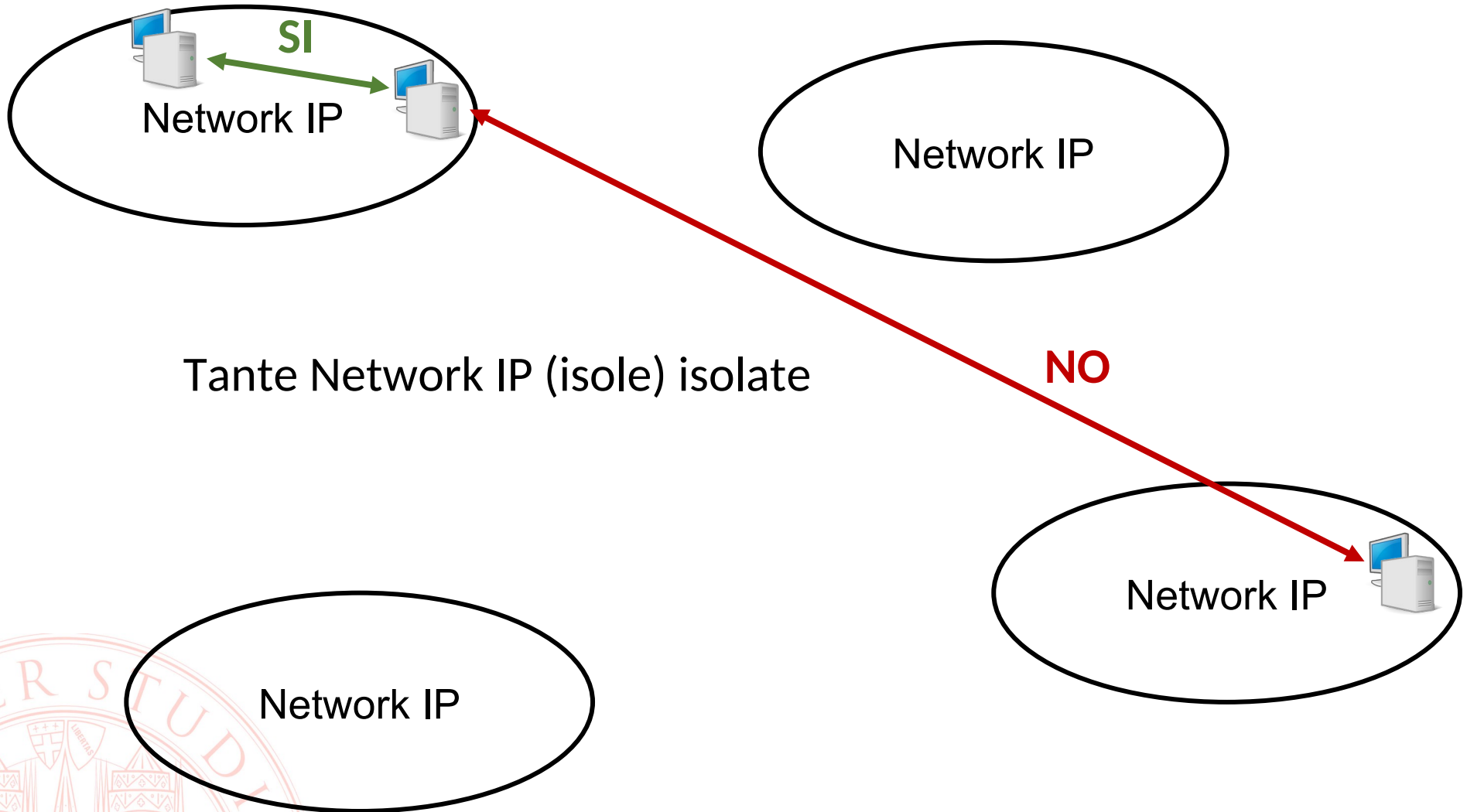
ARP reply - unicast



ARP reply - unicast



Internet: reti di reti



Interconnettere le isole

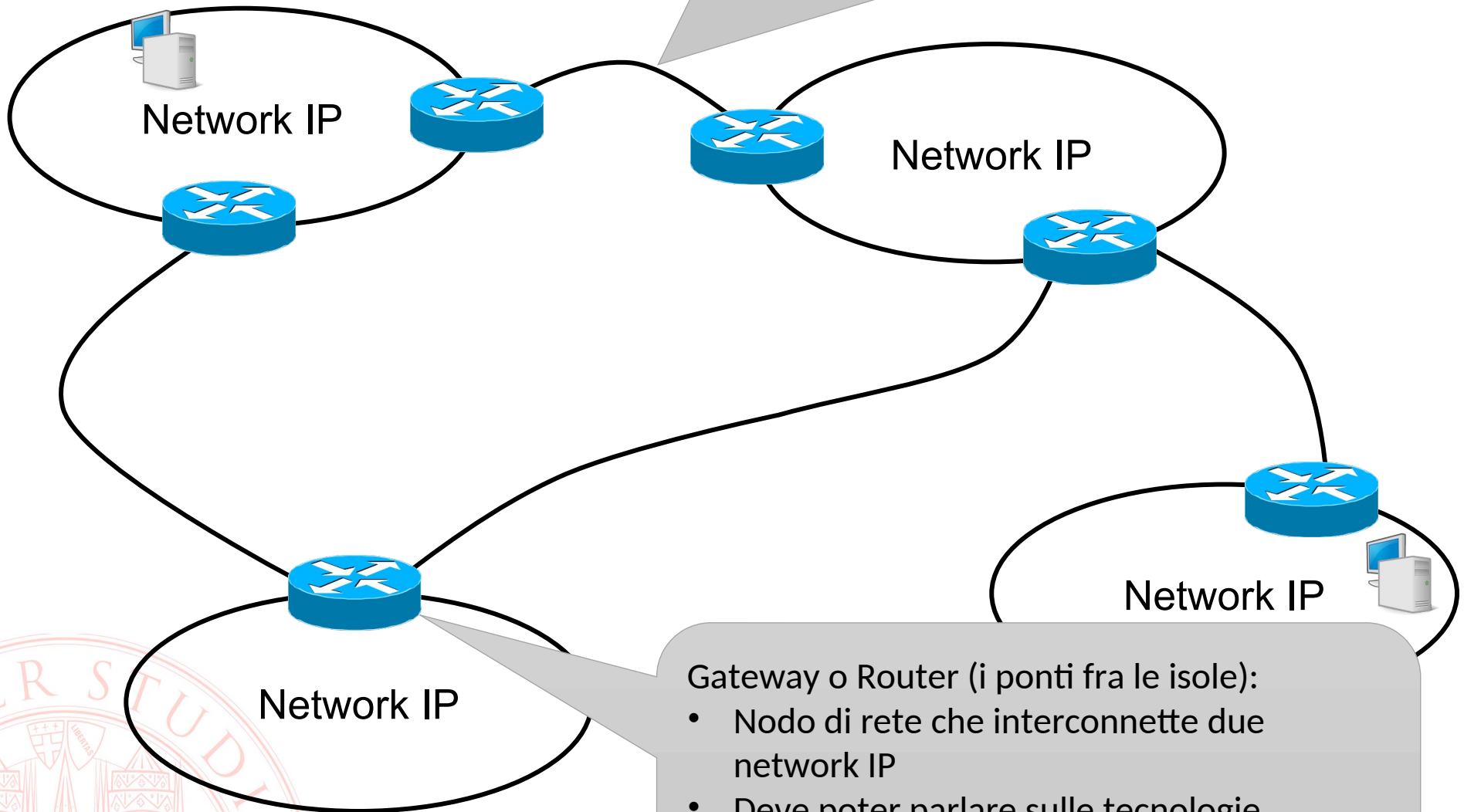
- Per far parlare tra loro le isole (network IP) è necessario che
 - Vi siano dei collegamenti fra le isole stesse, spesso realizzati con tecnologie diverse da quelle dell'isola
 - Vi siano degli apparati che permettono di usare questi collegamenti nel modo opportuno
 - Sia possibile scegliere il giusto collegamento verso l'isola che si vuole raggiungere



I router

Collegamento fra router:

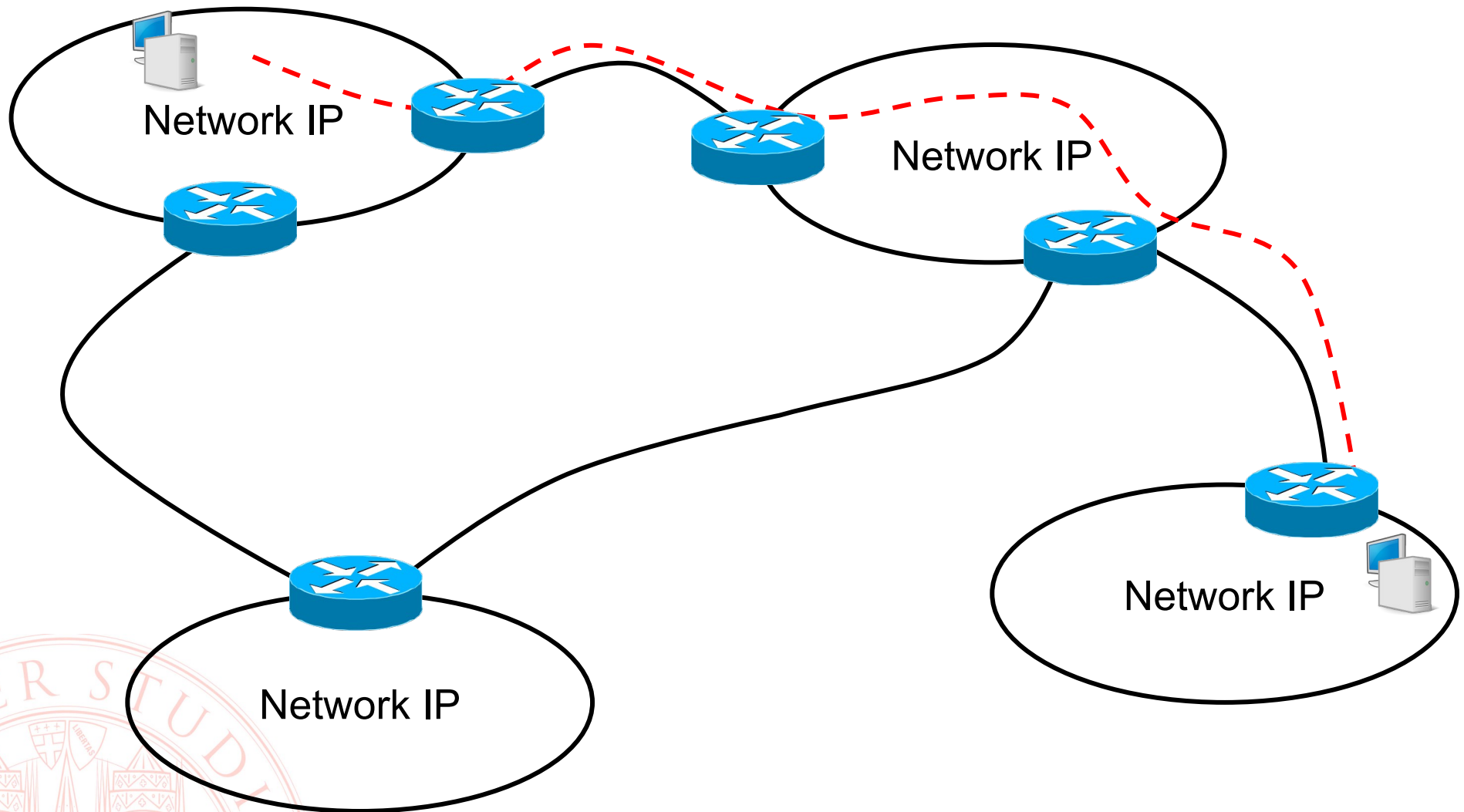
- Può essere una tecnologia simile a quella delle network oppure molto diversa



Gateway o Router (i ponti fra le isole):

- Nodo di rete che interconnette due network IP
- Deve poter parlare sulle tecnologie specifiche delle due Network
- Ha funzioni dal livello 1 al livello 3 OSI

Il percorso end-to-end

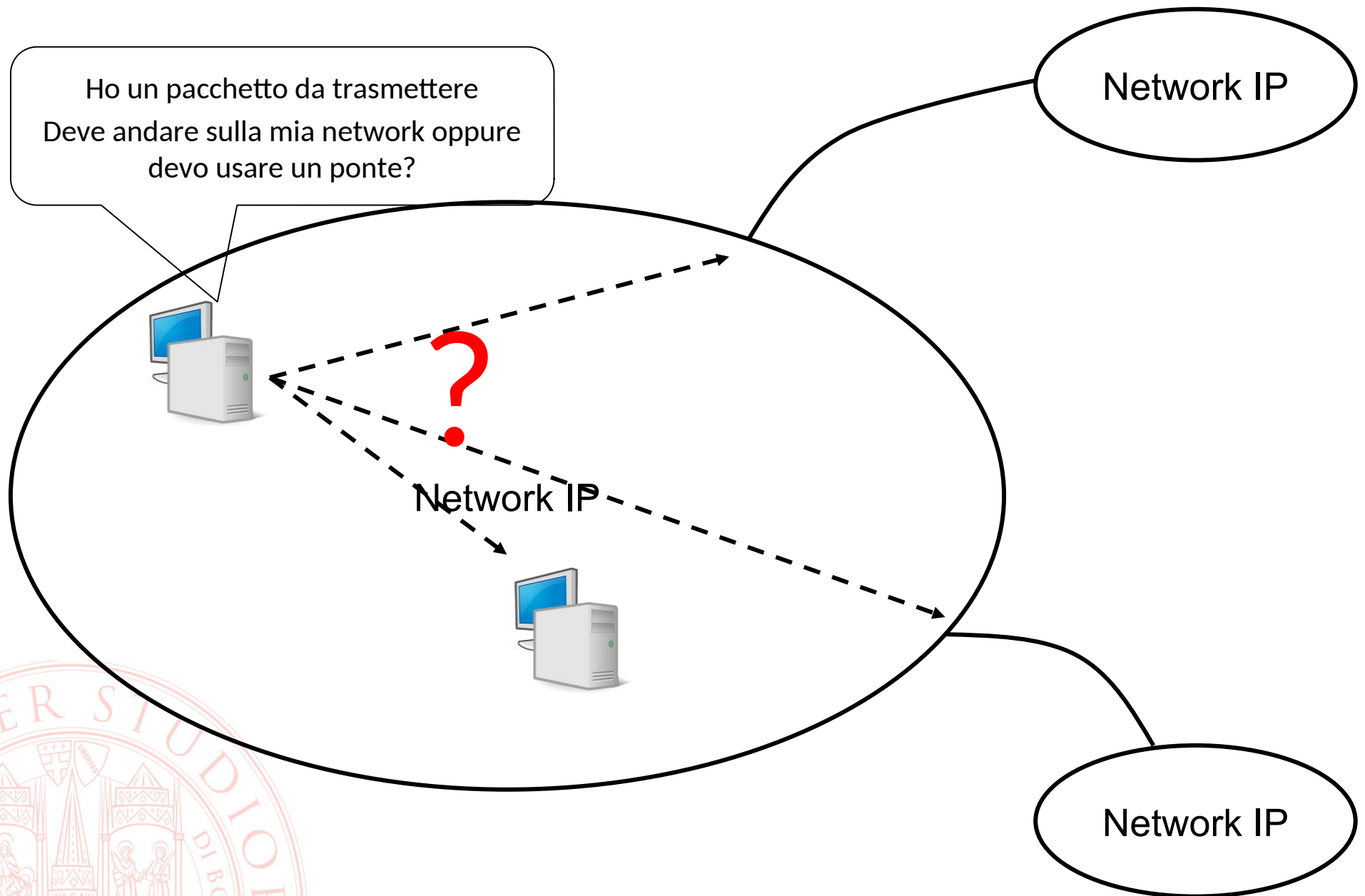


Cosa fa IP

- La tecnologia IP è agnostica rispetto alla tecnologia con cui sono realizzate le network
 - Il protocollo IP è concepito per lavorare indifferentemente su tecnologie diverse
- L'obiettivo di IP è quello di rendere possibile il dialogo fra network a prescindere dalla loro implementazione e localizzazione



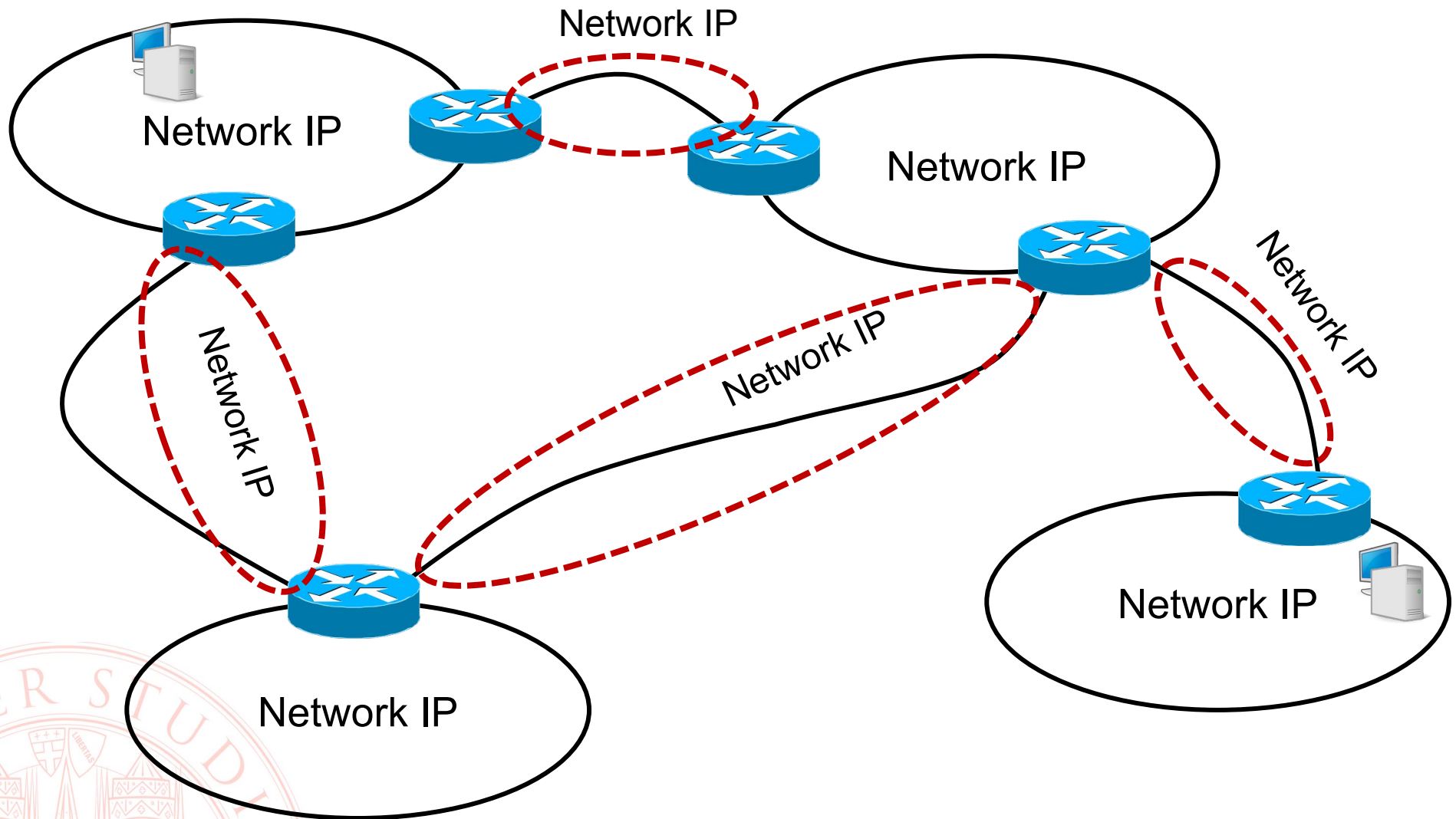
La domanda cruciale



La risposta

- Ogni nodo di Internet ha una base dati di destinazioni possibili
- Quando deve inviare un datagramma
 - Parte dall'indirizzo IP di destinazione
 - Legge la base dati
 - Decide quale azione intraprendere
- La tecnologia della propria network può essere utilizzata:
 - Per raggiungere la destinazione finale
 - Per raggiungere il primo ponte da attraversare

Le network fra i router

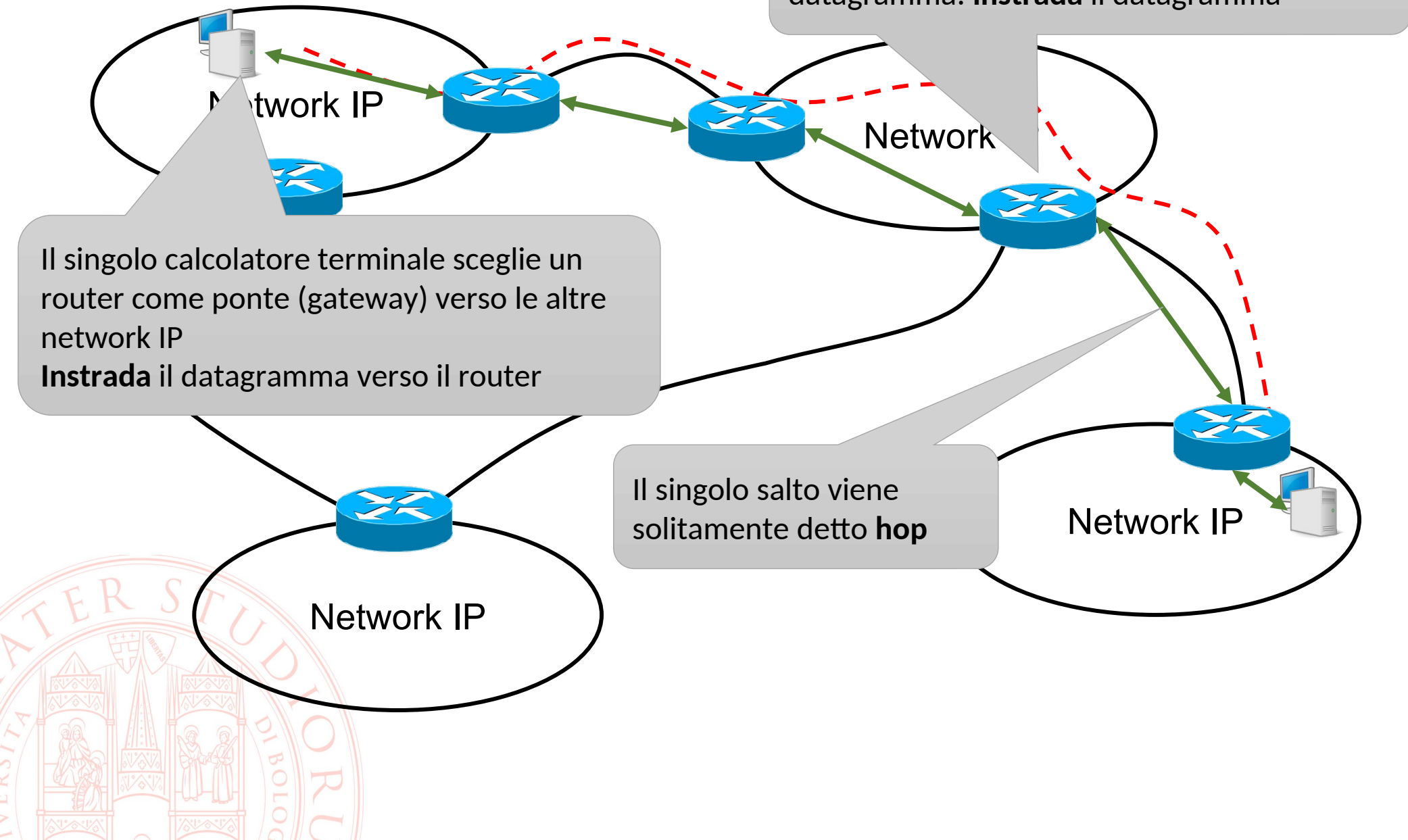


L'instradamento IP

Il router decide in che direzione inviare il datagramma: **instrada** il datagramma

Il singolo calcolatore terminale sceglie un router come ponte (gateway) verso le altre network IP
Instrada il datagramma verso il router

Il singolo salto viene solitamente detto **hop**



Instradamento diretto e indiretto

■ **Routing** : scelta del percorso su cui inviare i dati

- i router formano struttura interconnessa e cooperante:
 - i datagrammi passano dall'uno all'altro finché raggiungono quello che può consegnarli direttamente al destinatario

■ **Direct delivery** :

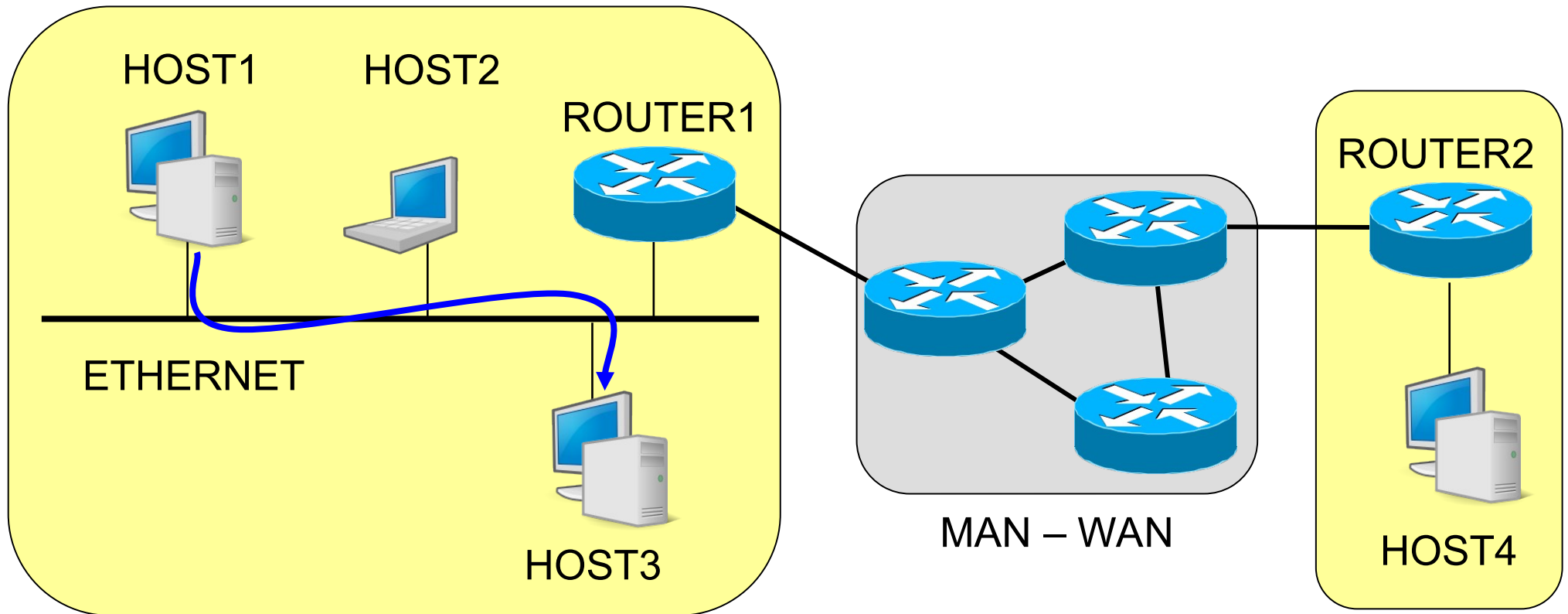
- IP sorgente e IP destinatario sono sulla stessa rete fisica
- L'host sorgente spedisce il datagramma direttamente al destinatario

■ **Indirect delivery** :

- IP sorgente e IP destinatario non sono sulla stessa rete fisica
- L'host sorgente invia il datagramma ad un router intermedio



Direct Delivery

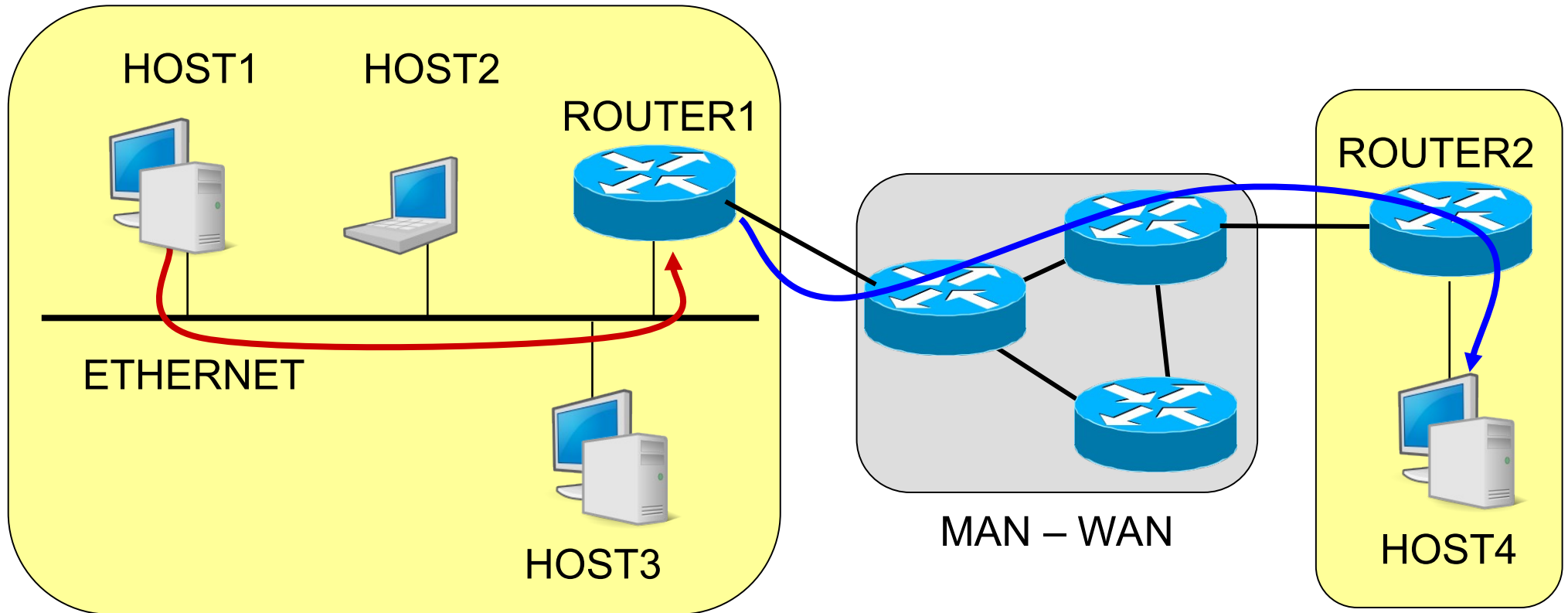


L2 ADDRESS: HOST3

IP ADDRESS: HOST3

DATI

Indirect Delivery



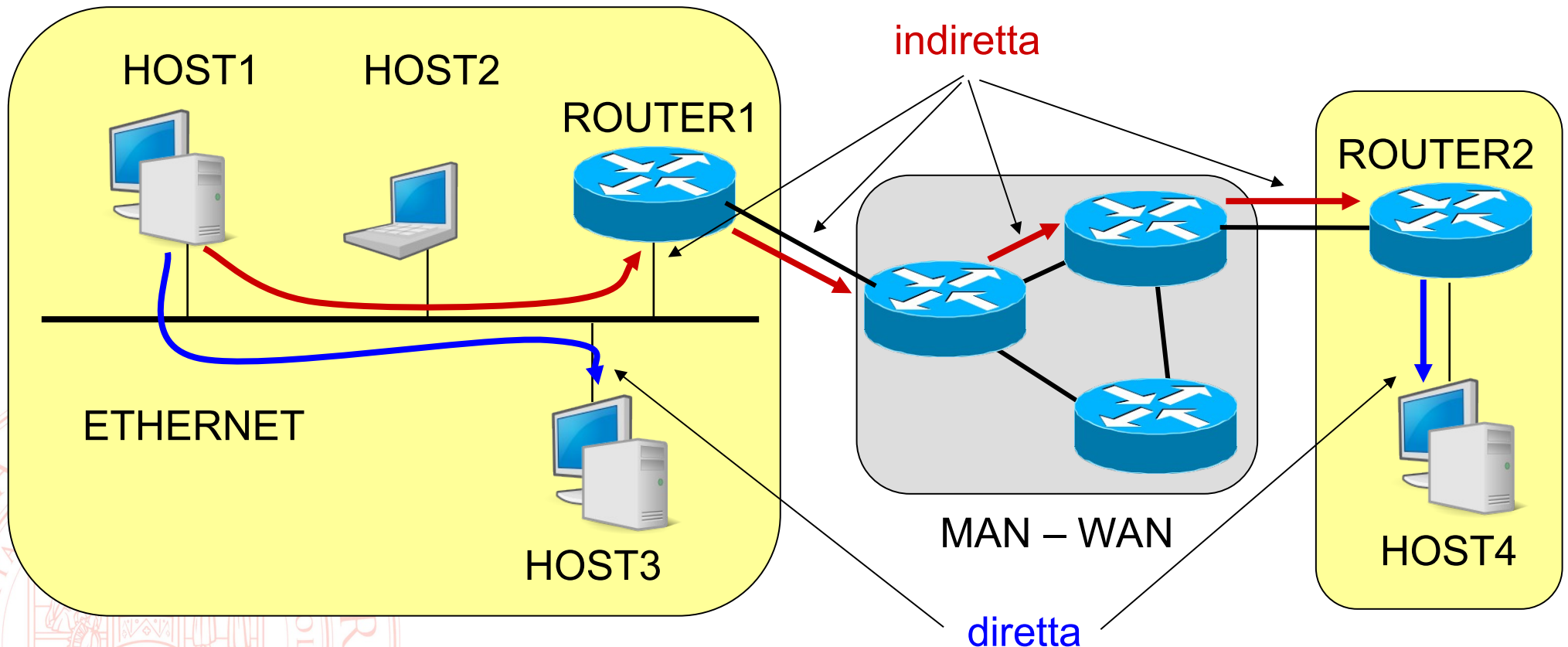
L2 ADDRESS: ROUTER1

IP ADDRESS: HOST4

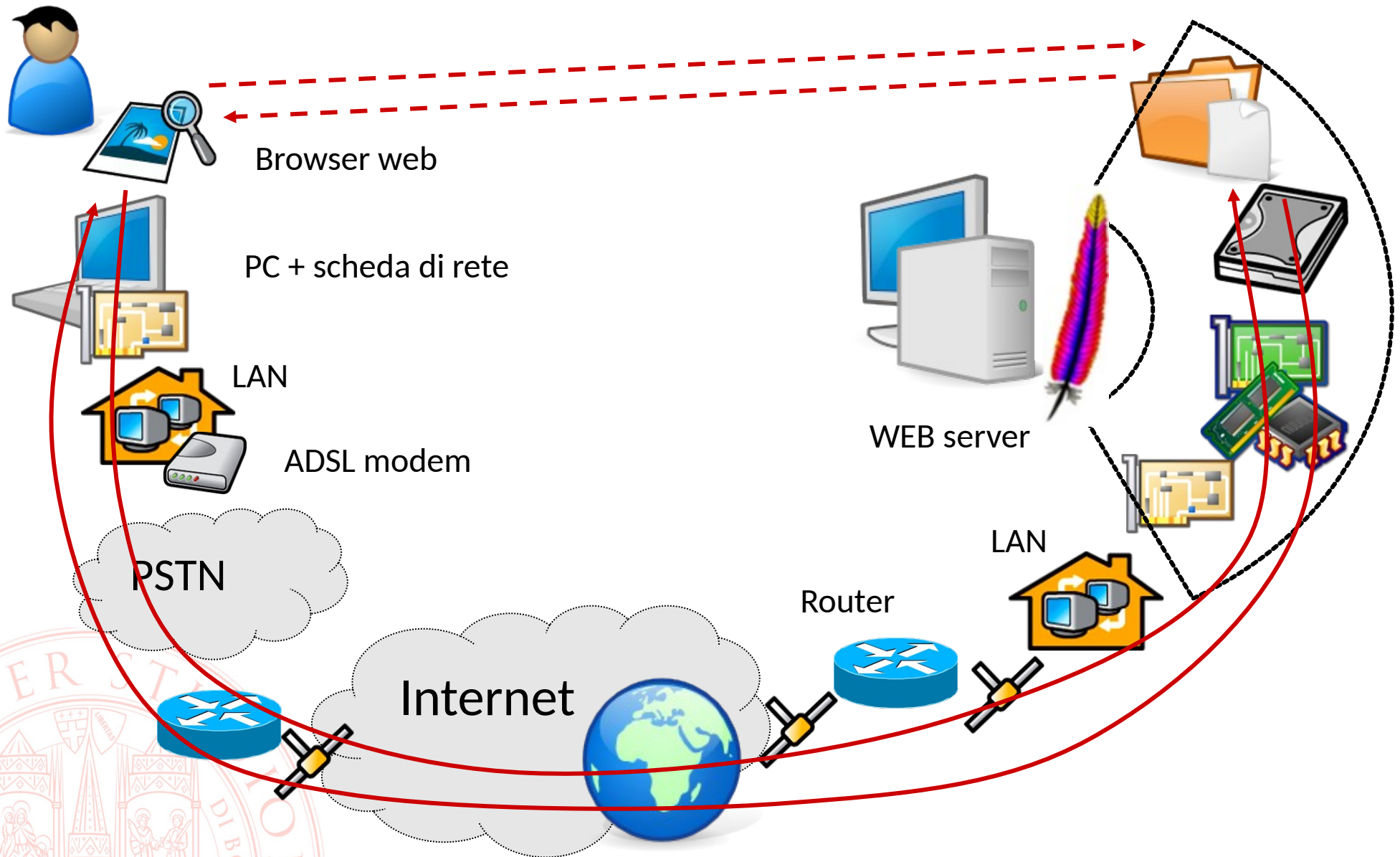
DAT1

Da mittente a destinatario

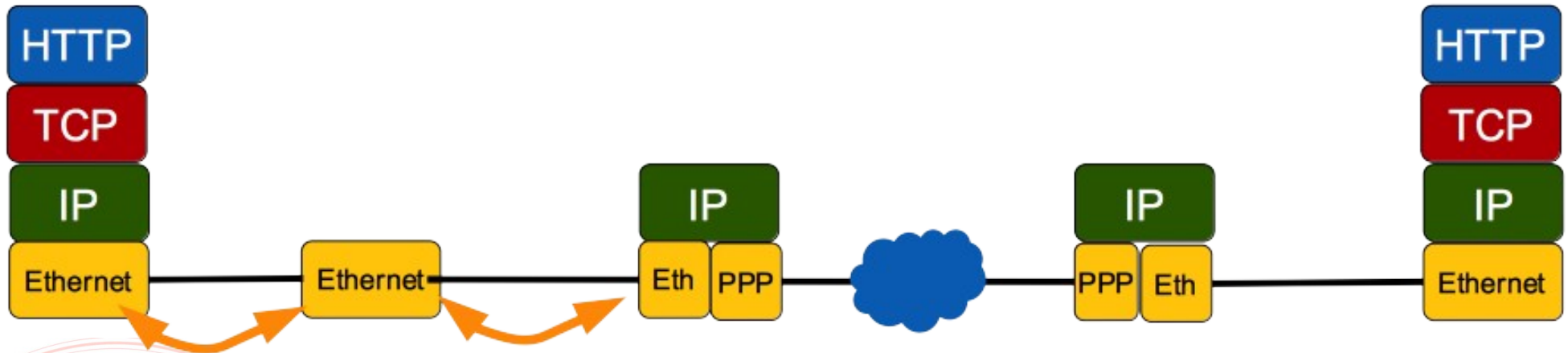
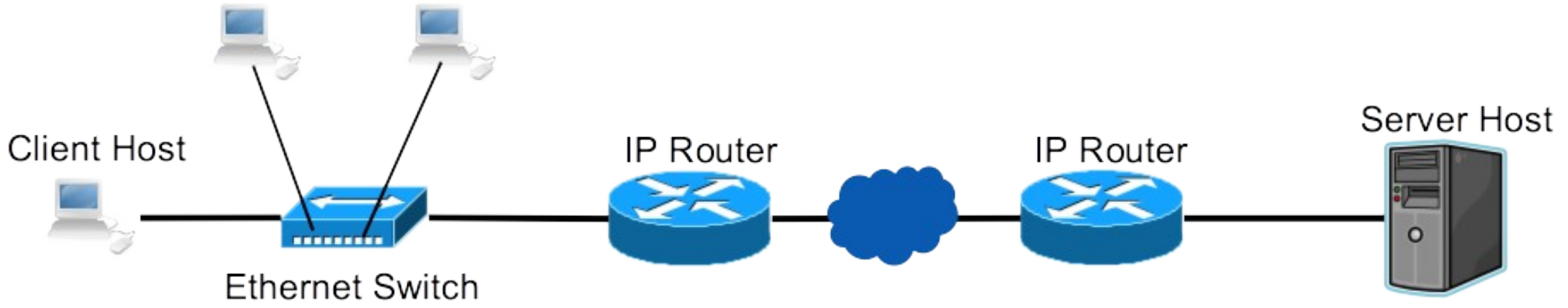
- C'è sempre una consegna diretta
- Può non esserci alcuna consegna indiretta
- Possono esserci una o più consegne indirette



Utilizzo di Internet: chi è coinvolto?



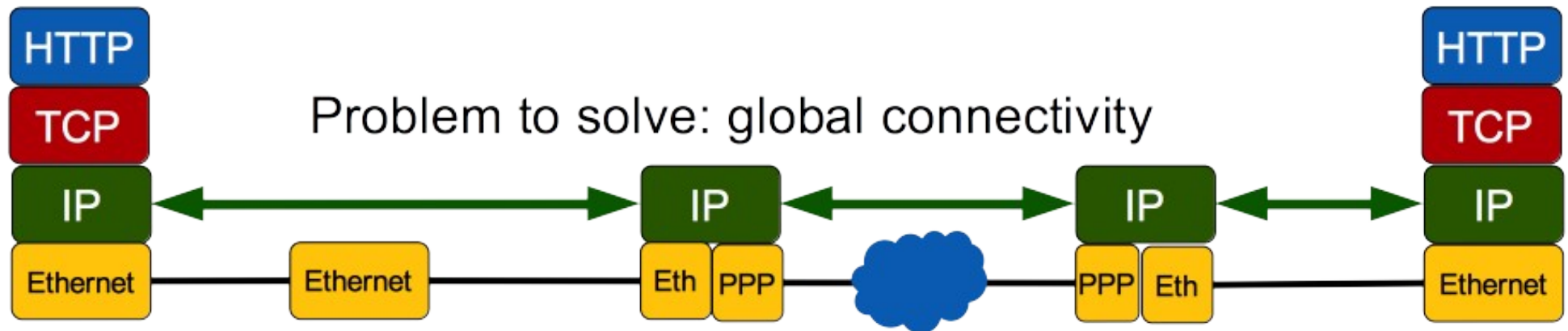
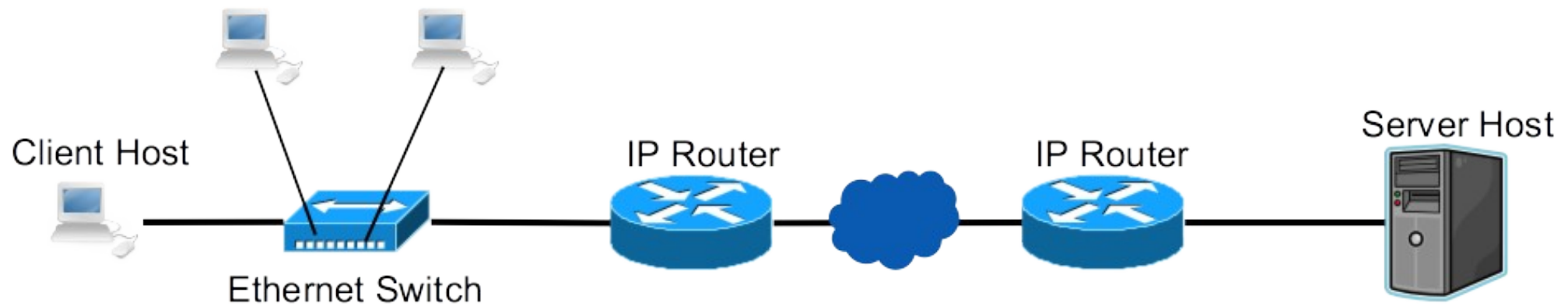
The Internet model



Problem to solve: local connectivity

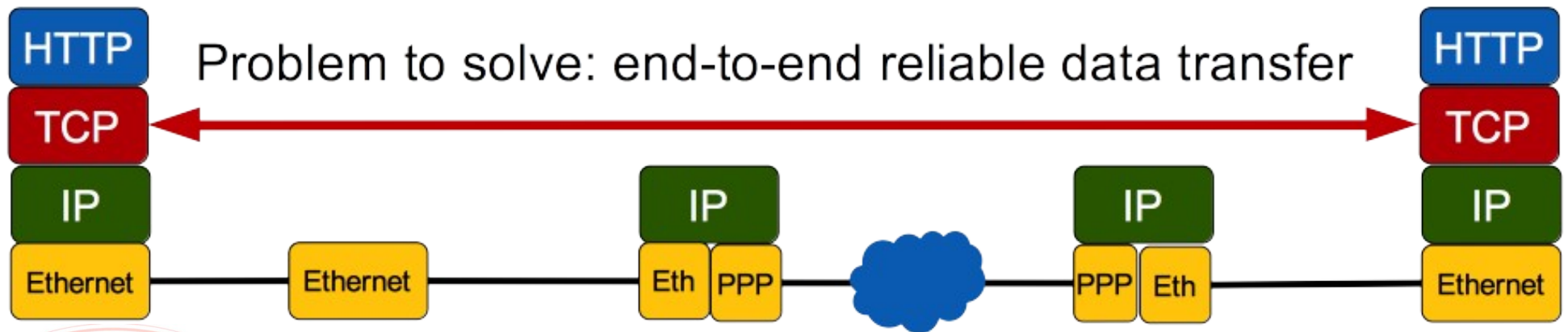
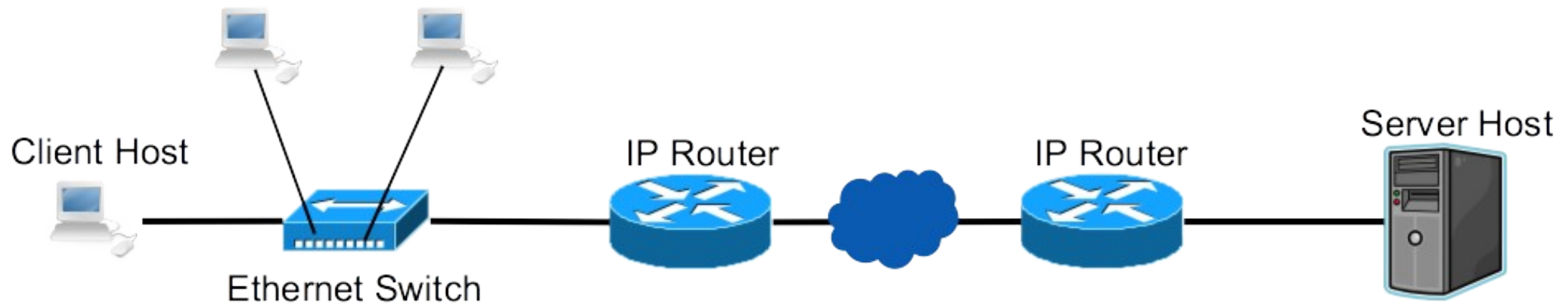
Security technologies: IEEE 802.1X, WPA2, Layer-2 VPNs

The Internet model



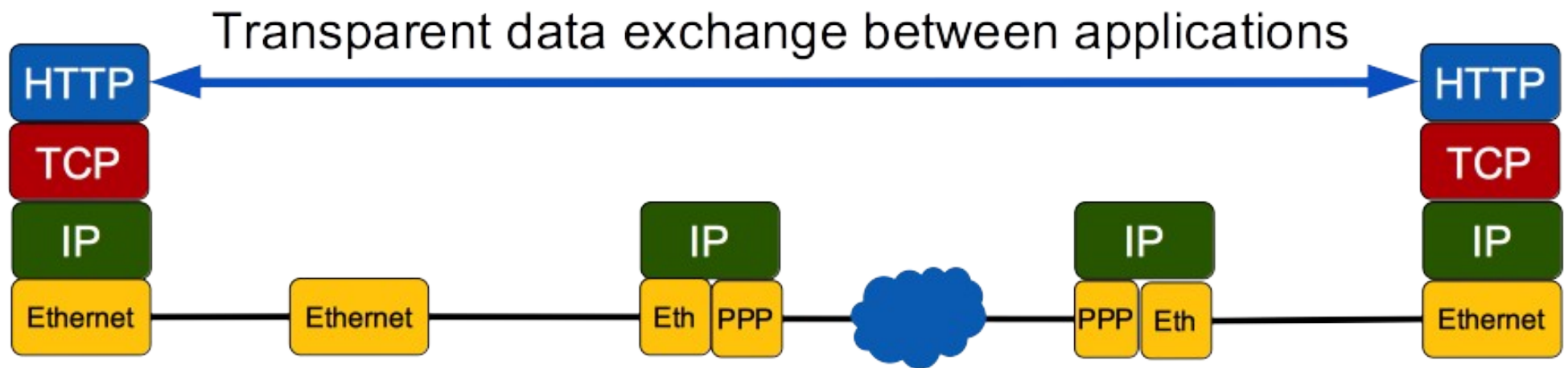
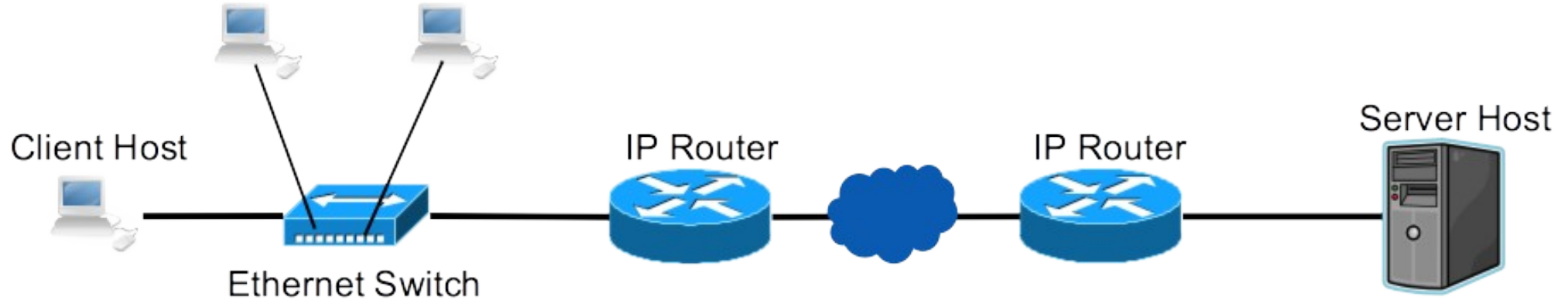
Security technologies: IPsec, Layer-3 VPNs, router authentication

The Internet model



Security technologies: SSL, TLS

The Internet model



Security technologies: authentication, crypto, application-layer VPNs, other application-specific solutions

Attacchi passivi

- Gli attacchi passivi non modificano i dati in transito
- Possono essere utili per l'aggressore e comunque dannosi per la vittima:
 - la **scansione** è uno dei primi passi della ricognizione
 - lo **sniffing** può compromettere la riservatezza dei dati
 - il **recupero di una chiave** consente di impersonare la vittima
- Utilizzati contro se stessi possono far parte di un vulnerability assessment (dettagli in seguito)



Scanning - esempi

■ Scansione di una rete

- indirizzi raggiungibili

■ Scansione di un host

- porte TCP / UDP aperte
- consente di dedurre le versioni del sistema operativo e dei servizi in esecuzione

■ "Loudness"

- per scopi VA, la scansione può essere aggressiva
- Gli strumenti implementano molti modelli di scansione silenziosa per eludere il rilevamento

```
prandini@disi057118:~$ nmap -sP 137.204.57.200-205
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-05 13:23 CEST
Nmap scan report for disi057204.ing.unibo.it (137.204.57.204)
Host is up (0.00064s latency).
Nmap scan report for dei057205.dei.unibo.it (137.204.57.205)
Host is up (0.00058s latency).
```

```
Nmap done: 6 IP addresses (2 hosts up) scanned in 0.21 seconds
```

```
prandini@disi057118:~$ nmap -A 137.204.57.104
```

```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-06-05 13:21 CEST
Nmap scan report for sia057104.ing.unibo.it (137.204.57.104)
Host is up (0.00020s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 3.0.2
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 47:17:ab:76:24:e2:6b:d6:25:cf:bf:c5:2b:30:e9:84 (DSA)
|   2048 69:a0:58:25:09:06:a6:9d:36:d6:56:b3:55:0e:4e:88 (RSA)
|   256 85:d9:53:e0:dd:ce:46:61:a8:cc:29:7f:a1:50:8d:3c (ECDSA)
|_  256 cf:a5:51:fa:f5:84:63:f8:d4:cf:00:90:bf:d5:9f:68 (EdDSA)
80/tcp    open  http     Apache httpd 2.4.7
|_http-server-header: Apache/2.4.7 (Ubuntu)
```

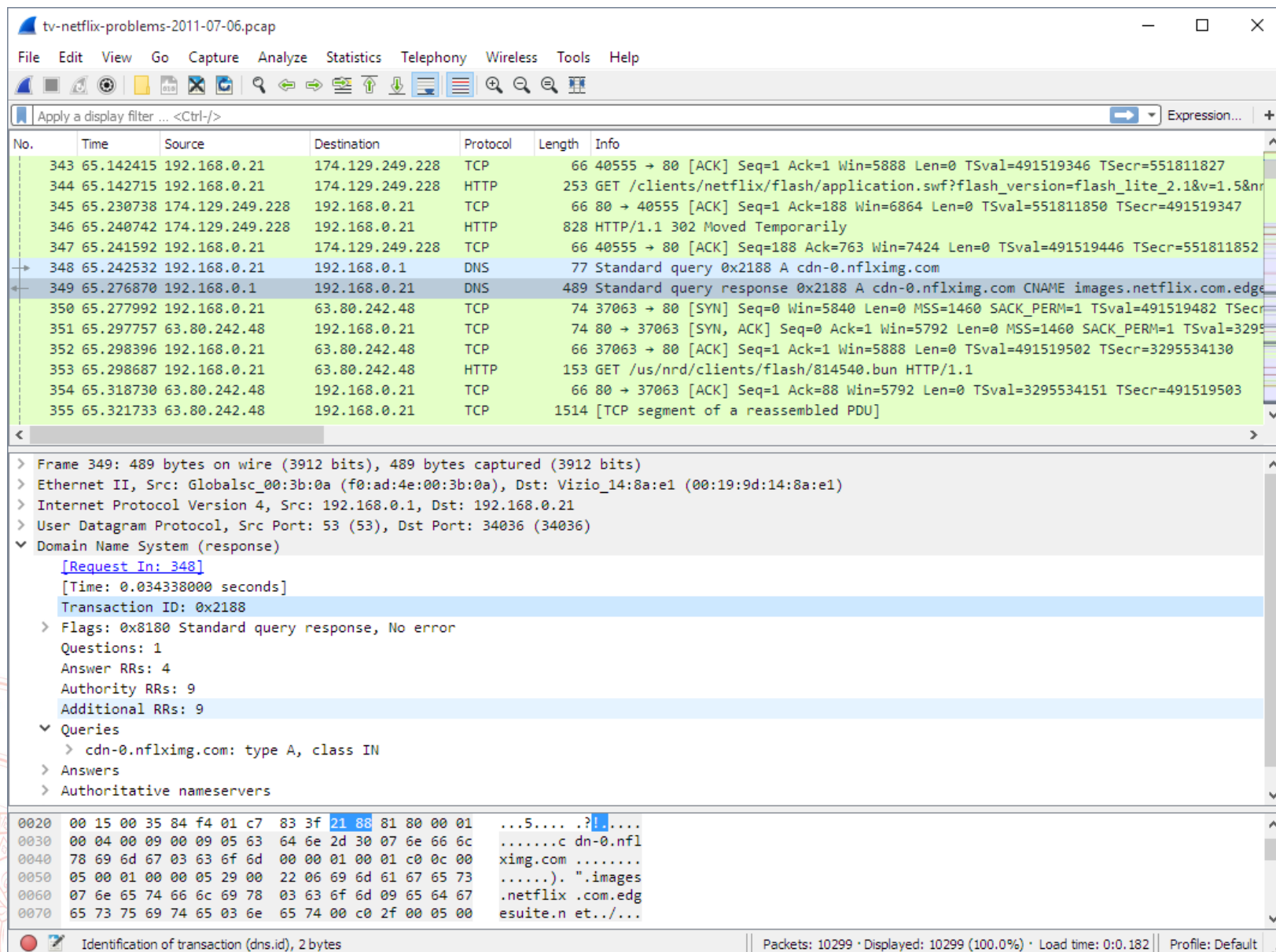
```
Service Info: Host: darma.ing.unibo.it; OSs: Unix, Linux; CPE:
cpe:/o:linux:linux_kernel
```

Sniffing

- **Lo sniffing richiede l'accesso fisico ai dati in transito**
 - essendo già sulla rete locale
 - a seguito di un attacco di dirottamento
- **Su reti locali**
 - wireless: tutto dovrebbe essere criptato, ma molti protocolli sono difettosi! (vedi seguito)
 - cablate: la crittografia esiste (802.1x per l'autenticazione delle porte, 802.1AE per la cifratura del traffico) ma non la usa quasi nessuno



Sniffing – un esempio



tv-netflix-problems-2011-07-06.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]

> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)

> Ethernet II, Src: Globalsec_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)

> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21

> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)

▼ Domain Name System (response)

[Request In: 348]

[Time: 0.034338000 seconds]

Transaction ID: 0x2188

> Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 4

Authority RRs: 9

Additional RRs: 9

▼ Queries

> cdn-0.nflximg.com: type A, class IN

> Answers

> Authoritative nameservers

0020 00 15 00 35 84 f4 01 c7 83 3f 21 88 81 80 00 01 ...5.... ?[.]....

0030 00 04 00 09 00 09 05 63 64 6e 2d 30 07 6e 66 6cc dn-0.nfl

0040 78 69 6d 67 03 63 6f 6d 00 00 01 00 01 c0 0c 00 ximg.com

0050 05 00 01 00 00 05 29 00 22 06 69 6d 61 67 65 73). ".images

0060 07 6e 65 74 66 6c 69 78 03 63 6f 6d 09 65 64 67 .netflix .com.edg

0070 65 73 75 69 74 65 03 6e 65 74 00 c0 2f 00 05 00 esuite.n et../...

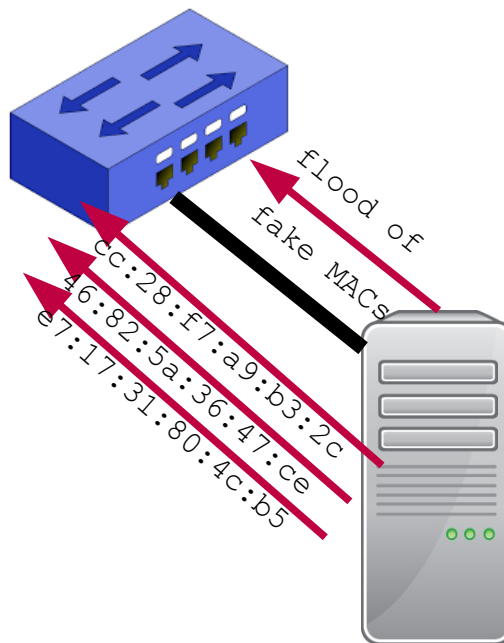
Identification of transaction (dns.id), 2 bytes

Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

MAC flooding

- Gli switch offrono una protezione limitata
 - idealmente, il traffico viene inviato solo sulla porta del destinatario
 - Se lo switch non trova un MAC nella CAM manda i pacchetti in broadcast
- Es. switch con CAM di dimensione 6 righe

Porta	MAC raggiungibile
1	eb:a6:99:de:1c:b0
1	2c:65:1e:b1:9f:44
3	0c:2e:22:b0:8e:16
4	5b:06:72:1b:3c:03
4	e4:b0:56:d5:2d:0f
4	92:ff:9e:6c:b0:8e



Porta	MAC raggiungibile
1	46:82:5a:36:47:ce
1	cc:28:f7:a9:b3:2c
1	e7:17:31:80:4c:b5
1	...
1	...other fake MACs
1	...

- Il MAC flooding costringe lo switch a comportarsi come un hub

Wireless key recovery

Ci sono quattro principali generazioni di protezione delle reti WiFi: WEP, WPA, WPA2, WPA3

■ WEP (Wired Equivalent Privacy)

- chiave simmetrica precondivisa
- stream cipher RC4, falla di progettazione: è possibile recuperare la chiave se viene raccolto sufficiente testo cifrato prodotto dalla stessa chiave
- la chiave è "randomizzata" da XOR con un IV piccolo (24 bit)
- generate abbastanza traffico e l'IV si ripeterà

■ WPA (WiFi Protected Access)

- una patch intermedia durante il lancio di WPA2
 - sostituisce IV con TKIP (128 bit)
- modalità personale con chiave precondivisa
 - nessuna segretezza in avanti: qualsiasi utente che conosce la chiave potrebbe decrittografare tutti i pacchetti
- modalità aziendale con autenticazione utente su canale protetto



Wireless key recovery

■ WPA2

- a lungo considerato essenzialmente sicuro
- grave vuln scoperta nel 2017: attacchi di reinstallazione chiave (KRACK)
 - Android e Linux possono essere indotti a (ri) installare una chiave di crittografia completamente zero
 - In altri dispositivi è comunque possibile decrittografare un gran numero di pacchetti
 - i pacchetti possono contenere credenziali utente con validità a livello aziendale!
- Pre-shared key (PSK) corta se si usa WPS

■ WPA3

- vari miglioramenti a garanzia della scelta di cifrari robusti
- sostituisce PSK con Simultaneous Authentication of Equals (SAE)
 - usa un sistema di handshake detto Dragonfly
- vulnerabile ad attacchi Dragonblood
 - tipo 1: sfrutta la retrocompatibilità con WPA2 – attacco MITM per forzare downgrade
 - tipo 2: sfrutta implementazione non corretta di alcuni passaggi crittografici – consente password partitioning
- dispositivi aggiornabili

Attacchi attivi

- **Gli attacchi attivi minacciano l'integrità, l'autenticità o la disponibilità di reti e sistemi**
- **Spoofing e hijacking sono spesso un passaggio preliminare per un attacco più impattante, ad es.**
 - rubare una rete per originare spam e scomparire
 - fingere un'identità di rete per rubare le credenziali
 - dirottare il traffico per fare sniffing
- **Denial of Service (DoS) rende inaccessibile un servizio**
 - ancora una volta come passaggio intermedio
 - ma anche come obiettivo principale



Link layer

■ Spoofing MAC

- assumere l'identità di un dispositivo a livello di indirizzo fisico
- molto efficace
 - per bypassare ACL
 - per ottenere tutto il traffico destinato alla vittima
- Limitato alla LAN
- tecnicamente facile da mitigare: 802.1x
(ma organizzativamente complesso → raro che lo si faccia!)



Link layer

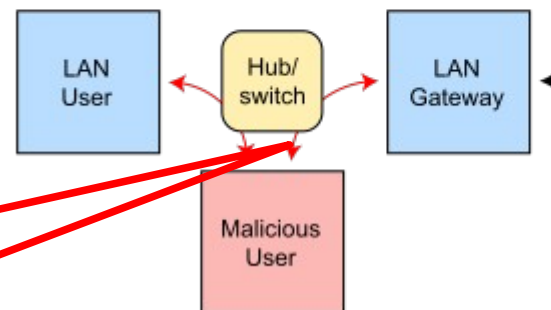
■ ARP poisoning

- convincere un host (specialmente il gateway) che l'IP di una vittima è associato al MAC dell'attaccante

Routing under normal operation



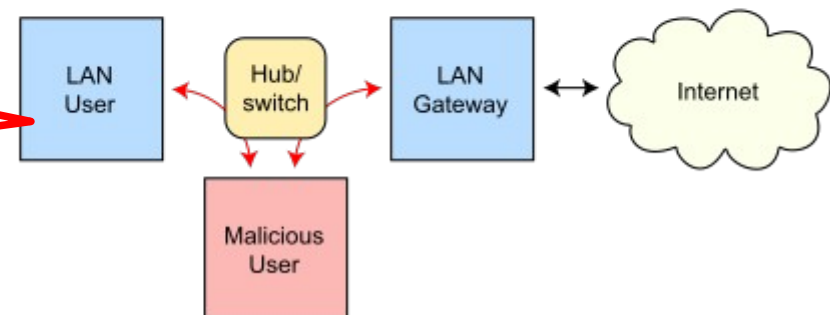
ARP poisoning



gratuitous ARP replies
“IP of gateway”
is at
“MAC of attacker”

Gli host usano la cache
“avvelenata” e mandano
sul cavo all’attaccante i
pacchetti per l’IP del gateway

Routing subject to ARP cache poisoning



Network layer

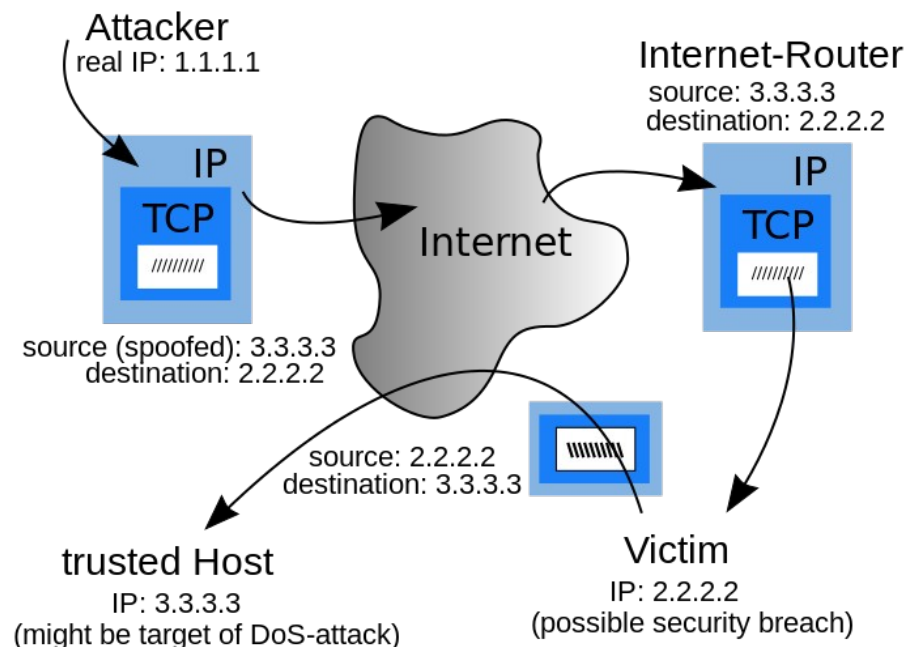
■ IP spoofing

- assumere l'indirizzo IP di una vittima
- efficace per dirottare il traffico solo su LAN
 - su Internet, il routing invierà le risposte agli indirizzi mimati
 - l'attaccante non può ottenerli
 - attacchi di *backscatter*! → →

■ IP hijacking

- i router si scambiano informazioni su come raggiungere le destinazioni
- BGP non è autenticato!
- Vedi alcuni esempi su <http://completewhois.com>
- estende la portata dello spoofing IP su scala globale

- Entrambi utili per bypassare ACL e per dirottare le connessioni dopo l'autenticazione (vedere più avanti)



By original by Nuno Tavares, svg-conversion by Loilo92, this version:GGShinobi - Own work, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=27991853>

Un caso famoso: Youtube & Pakistan Telecom

Dalla presentazione di Pilosov e Kapela a DEFCON16 (Las Vegas 2008)

- YouTube announces 5 prefixes:
- A /19, /20, /22, and two /24s
- The /22 is 208.65.152.0/22
- Pakistan's government decides to block YouTube
- Pakistan Telecom internally nails up a more specific route (208.65.153.0/24) out of YouTube's /22 to null0 (the routers discard interface)
- Somehow redists from static → bgp, then to PCCW
- Upstream provider sends routes to everyone else...
- Most of the net now goes to Pakistan for YouTube, gets nothing!
- YouTube responds by announcing both the /24 and two more specific /25s, with partial success
- PCCW turns off Pakistan Telecom peering two hours later
- 3 to 5 minutes afterward, global bgp table is clean again

<https://virtuale.unibo.it/mod/uniboresh/view.php?id=538071>

<http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf>

Layer di trasporto e applicazione

- Se il dirottamento IP viene utilizzato per impossessarsi di una connessione dopo un'autenticazione, devono essere coinvolti i livelli superiori
 - UDP è privo di connessione: molto facile

invece

 - TCP perderà la connessione se l'attaccante non utilizza i numeri di sequenza corretti per la finestra scorrevole
 - Spesso i protocolli a livello di applicazione utilizzano identificatori di sessione come i cookie HTTP
- In entrambi i casi l'attaccante ha due opzioni
 - indovinare (forza bruta, spesso molto difficile)
 - sfruttando lo sniffing (se già sul percorso dei dati)



(D)Dos

■ Qualsiasi attacco dirottamento può causare un errore mirato

- livello di trasporto: l'invio di un SN errato o un reset esplicito su connessioni TCP li interrompe

■ Distributed Denial of Service

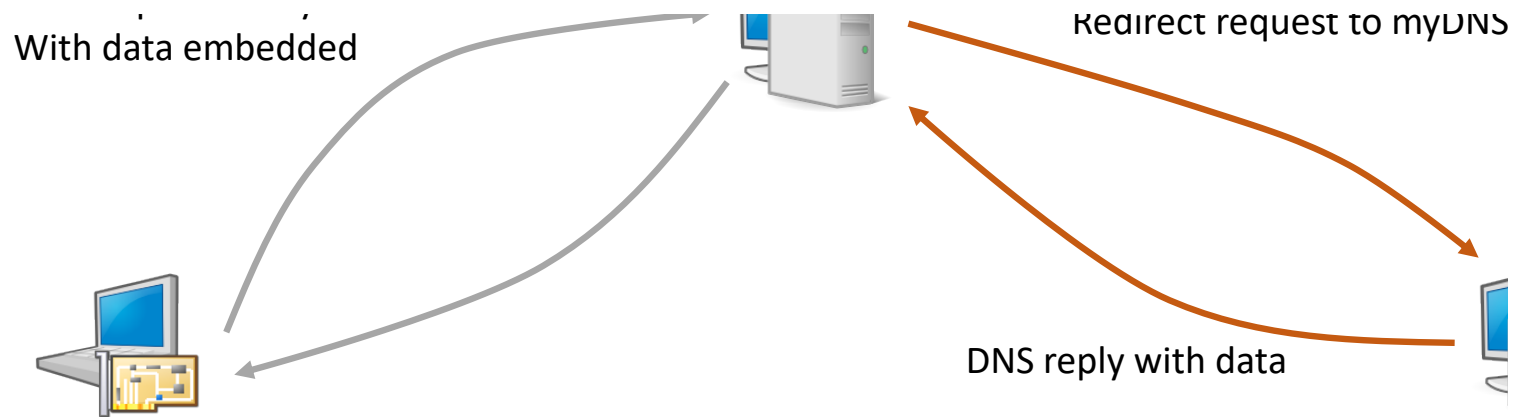
- molti host coordinano i loro sforzi per saturare la capacità di rete o le risorse di calcolo della vittima
- Le **botnet** sono insiemi di computer zombie che possono lanciare attacchi DDoS quando istruiti da comando e controllo (**C&C**)
 - Botnet IoT: Mirai, Bashlite, ...

■ un controllo degli accessi impreciso sull'infrastruttura può peggiorare le cose

- in termini di effetto
- nascondendo l'origine
- per esempio: attacchi di amplificazione DNS

Un esempio di esfiltrazione: DNS Tunnelling

- Query e risposte possono contenere dati
- Utilizzabile per esfiltrare dati da un computer infettato o per mettere in contatto un bot con il C&C



Protocolli ausiliari: DNS hijacking

- Un server DNS malevolo può fornire in risposta l'IP dell'attaccante quando viene richiesto dalla vittima di risolvere un nome legittimo
- DNS
 - non è autenticato
 - è distribuito
 - ha molti livelli di memorizzazione nella cache
- La falsificazione arbitraria è difficile ma ...
 - vedere più avanti per un attacco combinato
 - i server legittimi possono essere attaccati e portati ad agire in modo malevolo



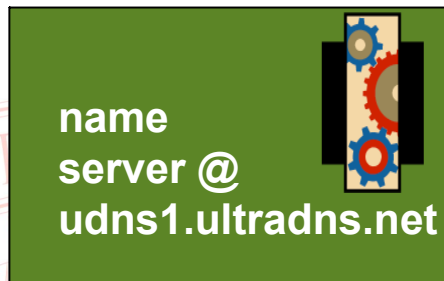
DNS spoofing

- Query e risposta normali

www.amazon.com?



207.171.166.48



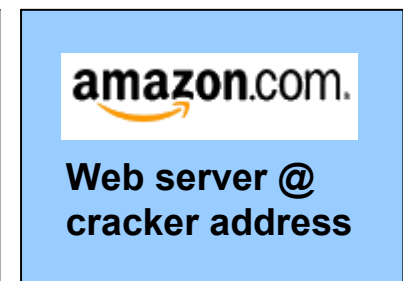
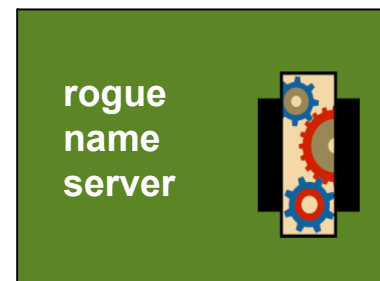
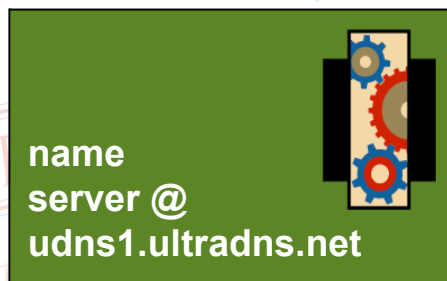
DNS spoofing

- Risposta falsificata

www.amazon.com?



~~207.171.166.48~~



cracker address

DNS spoofing (pharming)

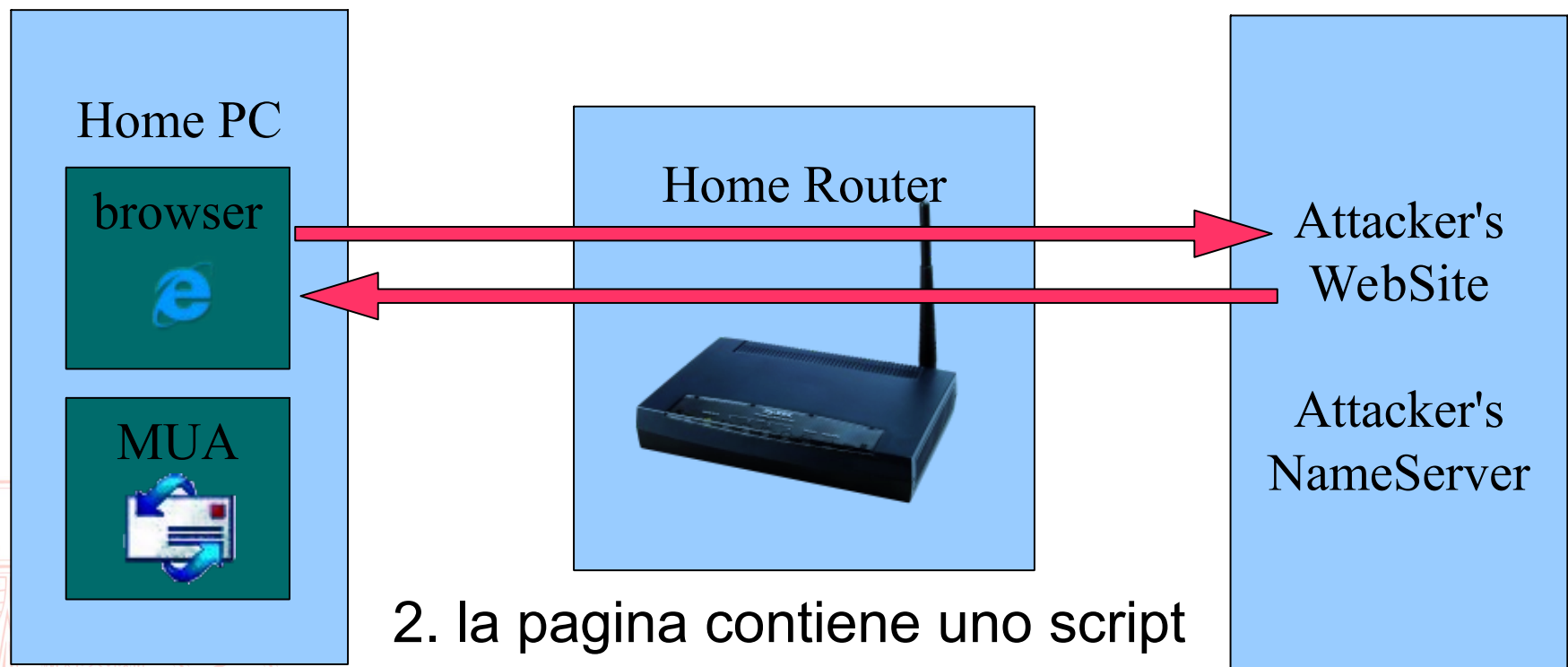
- Sembra difficile falsificare una risposta DNS?



1. L'utente visita una pagina HTML, consapevolmente o no

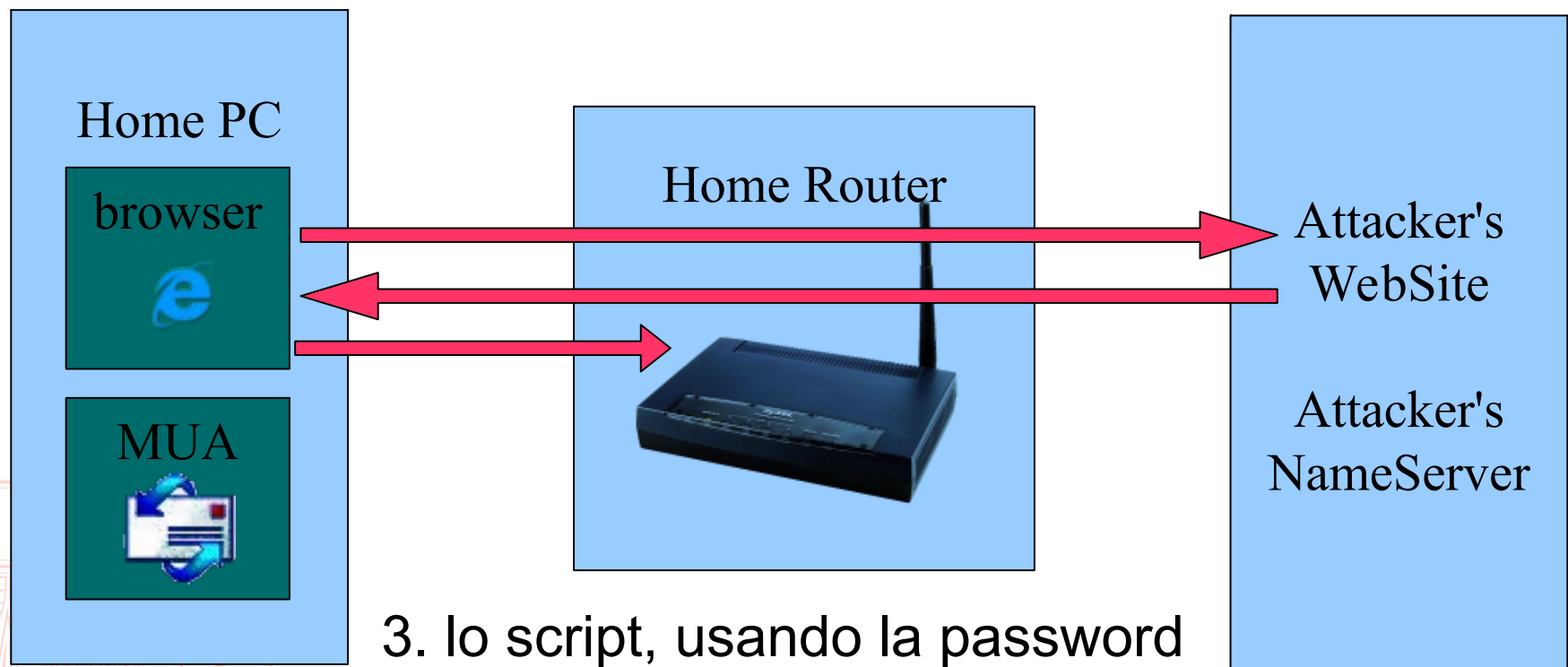
DNS spoofing (pharming)

- Sembra difficile falsificare una risposta DNS?



DNS spoofing (pharming)

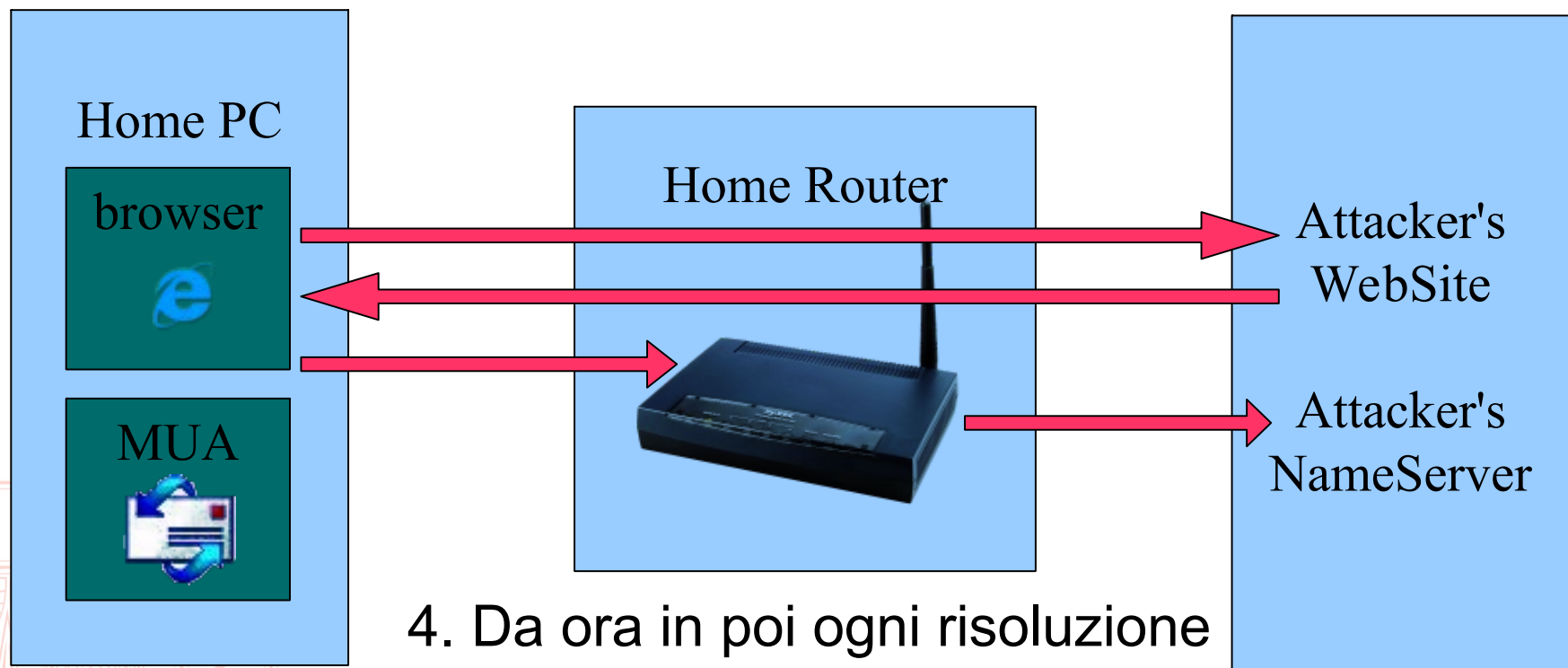
- Sembra difficile falsificare una risposta DNS?



3. lo script, usando la password di default del router, riprogramma il DNS

DNS spoofing (pharming)

- Sembra difficile falsificare una risposta DNS?



4. Da ora in poi ogni risoluzione sarà eseguita dal NS dell'attaccante